MINUTES IACR BOARD MEETING *VIRTUAL-10 '20*

16 DECEMBER 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 21 full time attendees with Batina holding proxy for Schwabe, Lepoint for Baldimtsi, Reyzin for Lysyanskaya, Yung for Preneel and Stebila for Paterson when they are not present.

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

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-9 '20.*

1.3. **Update about 2021 BoD changes.** The President recalls this is the last Board meeting for Kwangjo Kim (*Asiacrypt'20* General Chair (2019-2020)), Leo Reyzin (*Crypto'20* General Chair (2019-2020)), and Kenny Paterson (Journal of Cryptology Editor-in-Chief 2017–2020, *RWC* Steering Committee). The President thanks them for all their great work during this difficult year.

Kenny mentions that a lot of progress has been made with respect to the old submissions and that the handover to Vincent Rijmen is going very smoothly.

2. Officer and Appointments (decisions and information)

2.1. **Proposal for Co-Editor in Chief for TOSC for 2022-2023.** The *FSE* Steering Committee proposes Bart Mennink (Radboud University, the Netherlands) as Co-Editor in Chief for TOSC (for *FSE* 2022-2023). The *FSE* Steering Committee requests the IACR Board to approve this proposal.

Decision 2 (unanimous)**.** *The Board appoints Bart Mennink as the Co-Editor in Chief for TOSC (for FSE 2022-2023).*

3. CONFERENCES

3.1. **Update on recent and forthcoming conferences (FSE / TCC / ASIACRYPT / RWC).** Halevi provides an update on *TCC'20*, this was a very successful event and a joined virtual workshop with *FOCS* took place. The *TCC* Steering Committee just approved *TCC 2021* and more information will be shared with the Board soon. For this virtual workshop it was *not* mandatory to become an IACR member (and pay the membership fee). McCurley recalls this meant that the links to the meeting rooms needed to be opened up. This is a potential risk for abuse which fortunately did not happen. In the future we should probably not organize it in this fashion.

Kim summarizes that *Asiacrypt'20* was a success. A highlight were the virtual break-out rooms in different languages. This worked really well and a lot of discussion and interaction took place.

Paterson mentions that they ran a survey for *RWC'21* to see what time worked best. Currently, the program is up and the registration is open. Since this is the first IACR event of 2021 participants need to pay their membership fee although the event is for free. This might have an impact on the attendance. Stebila mentions that for *Crypto* more than half of the registrations occurred in the last two weeks. McCurley notes that they plan to experiment with more interaction. From past events it became clear that senior members do not engage a lot in the social aspects of the virtual event. *RWC* is working on new ways to encourage social interaction. A small demo of the new features is given to the Board. Paterson thanks McCurley for this great work and really likes the new features.

3.2. **Discussion about 2021 conferences.** The President thinks it will still be a while before we are back to a somewhat normal situation. He starts a discussion about the best approach for conferences in early 2021. What should we do about *Eurocrypt* which is scheduled for May 2021: we could shift this to the fall or stick to the original schedule. Batina recalls this has been discussed in the emergency meeting. The fall has a better chance for a partial physical participation. A possible date would be sometime in October. She asks the opinion of the Board.

Halevi likes the idea of hybrid conferences. This is a good idea for our future by itself. We should define a threshold for the number of people attending such that organizing the physical event makes sense. His feeling is that everything above 100 physical participants might be fine. McCurley agrees, many people might not be allowed to travel by May. The hybrid model is a good thing to try. We should not only consider how many attendees can make it but also how many speakers will show up in person to the event. Heninger mentions that *CCC* is a good example of a hybrid event. She thinks that an event with 100 people might be practically feasible but is irresponsible. As a data point, UCSD has banned all in-person events through May 31, 2021.

Organizing *Eurocrypt* in October sounds good to McCurley. We should consider releasing papers at the original date. Preneel agrees, organizing this in May is too soon: fall is the better option. The President is also in favor of hybrid events, he concludes that most people think May is not realistic. He suggest to lock-in the dates for October. McCurley asks Batina if she prefers to do this virtually in May. Batina likes this proposal of organizing the event in October. Stebila foresees that the fall will be extremely busy with all postponed events if things get back to a more normal situation.

LaMacchia comments that for *CHES'21* we are committed to the hotel in Beijing in September with standard cancellation costs: this event will likely happen. Reyzin remarks that the virtual events have received very positive feedback so far. We should organize and collect our lessons learned and avoid going back to how we used to run our physical conferences. We should keep the positive aspects of the virtual events and incorporate them in the physical events.

Halevi mentions that we should be willing to risk some of the IACR budget when signing contracts. The health of our community is the number one priority and we should not be afraid to cancel events. The Treasurer fully agrees with this statement. We have the reserves and could even get this back from future events.

Abe mentions that we should ensure the chronological order of publication. When events are shifted it might happen that follow-up work appears before the original paper appears. Yung suggests to publish proceedings in chronological order even when events are shifted.

4. TOPICS

4.1. **Policy for resubmissions across different conferences.** Some of the security conferences such as *Usenix* have a submission policy which requires authors to show previous reviews and how this was addressed in an appendix to the submission. The President asks the Board about opinions and would like to discuss this in more detail if this is something the IACR should consider.

Yung summarizes his experience which was negative although in principle this approach might work. In his case the reviewers were lazy and simply copied over the old reviews even when the paper had been updated. Standaert mentions this also depends on the type of reviewer comments: technical, editorial or taste. Heninger mentions she had a positive experience as a reviewer with this approach. It would be good to make the reviews only available to the reviewers after writing and submitting your own review. The revision system by moving to

multiple deadlines a year in the security community has been a very good experience. We have an opportunity to create a revision process across all IACR conferences.

Preneel recalls that both *FSE* and *CHES* already have such rebuttals. However, we will always have the situation that some authors just ignore comments and some reviewers are lazy. We should be careful not to create new problems by solving these ones. Reyzin remarks that in the long run the approach from *CHES* and *FSE* might be good for all venues. In the short run, however, we should not have past reviews available before we submit a new review; we first need the software available which can support this. McCurley fully agrees that this is also a technical challenge, especially when we aim to implement this across different conferences. Fischlin remarks that old reviews often do not make sense anymore because the paper has been updated significantly and the older version is not available. Heninger suggests to maybe create two different submission tracks: one for fresh and one for resubmissions.

4.2. **New journal proposal update.** Bos provides an update on the work the New Journal Committee has been done. All is going as planned and progress is being made. The aim is to provide the Board with a larger update in Q1 of 2021.

5. Closing Matters

Abdalla closes the meeting at 18h04 CEST.