# MINUTES IACR BOARD MEETING *VIRTUAL-1 ’21*

21 JANUARY 2021

## 1. Opening Matters

1.1. **Welcome, roll of attendees, identification of proxies.** At 22h03 CEST Abdalla opens the meeting and briefly goes around for an introductory round, confirming attendees and establishing who is holding proxies. There are 20 full time attendees with LaMacchia holding proxy for Heninger and Halevi for Lysyanskaya when she is not present. Batina leaves at 23h17 and Schwabe has her proxy.

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 2021-2023); Marc Fischlin (Director 2020-2021); Tancrède Lepoint (Director 2021-2023); 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 2021-2023, *PKC* Steering Committee).

*Attendees* (Appointed). Foteini Baldimtsi (Communications Secretary (2019-2022)); Lejla Batina (*Eurocrypt’20/’21* General Chair (2019-2021)); Allison Bishop (*Crypto’22* General Chair (2021-2022)) Colin Boyd (*Eurocrypt’22* General Chair previously *Eurocrypt’21* General Chair (2020-2022)); Jian Guo (*Asiacrypt’21* General Chair (2020-2021)); Vladimir Kolesnikov (*Crypto’21* General Chair (2020-2021)); Douglas Stebila (Membership Secretary (2017-2022)); Bo-Yin Yang (*Asiacrypt’22* General Chair (2021-2022)).

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

*Absentees* (Elected). Nadia Heninger (Director 2019-2021).

*Absentees* (Appointed). Vincent Rijmen (Journal of Cryptology Editor-in-Chief 2021–2023).

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

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-10 ’20.*

1.3. **Review of open action points.** Bos provides an overview of the open action items. Currently, only three items from last year are still open which are discussed with the Board.

- From 2020-virtual-1 (Halevi): Provide the scripts which automatically create a new websubrev instance to McCurley.
  Neither Halevi nor McCurley recall if this happened or not. They will check and address this. Action item can be closed.
- From 2020-virtual-8 (President): Ask Yu about his recommendation on how to best share videos in Asia.
  This is on the agenda today.
- 2020-virtual-9 (President): Propose the way forward for the Test-of-Time Award for older papers.
  This is on the agenda today.

## 2. Conferences

2.1. ***TCC 2021* Proposal.** Halevi explains the proposal to hold *TCC 2021* in November in Raleigh, North Carolina, USA. This is with the same organizers as *TCC 2020* which happened virtually. This year it is not co-located with *FOCS*.

McCurley asks about the considerations to organize this as a hybrid event. Is there local support for cameras and someone dealing with IT issues, what are the additional costs and how do we ensure the event is streamed and recorded? This event would be a good candidate for a hybrid event. Stebila suggests to extend the template for the conference budget to add a line item for such additional costs related to hybrid events. The President agrees and this *TCC* budget needs to be revised to take the possibility of a hybrid event into account. There follows a discussion how and when the Board should decide to turn this event in a hybrid conference. The current proposal ask for physical conference, the Board can always decide to go hybrid later. The President agrees and we should inform the General Chair of the possibility to convert this to a hybrid event and we need to verify if the General Chair is comfortable with this decision. The Treasurer would like to see an add-on to the proposal which takes the estimated costs for a hybrid event into account.

**Decision 2** (unanimous)**.** *The Board approves the proposal for TCC'21 in Raleigh, North Carolina, USA, selected by the TCC Steering Committee with General Chair Alessandra Scafuro and Program Chairs Kobbi Nissim and Brent Waters.*

2.2. **Eurocrypt 2021.** The President recalls the discussion at the last Board meeting that a physical event in May is not possible. We can go virtual or shift this to October. Batina already locked end of October as tentative dates. It is her preference to have a physical *Eurocrypt* if we can guarantee a minimum number of attendees. Standaert mentions that the slots for the accepted papers have been selected as if this was a physical conference: what should they put in the notification? The President wants to consider all risks: Europe might indeed be better in October but it might be difficult to attend from outside Europe. It is almost certain fewer people will attend. The President has reservations and asks the Board for their opinion. Yung thinks it is good to fix these dates with the intention to have a partial physical event. We can always change when needed. There should not be a delay in the publication of the proceedings. The President confirms that the publication schedule is not affected. Batina checked with the venue and a hybrid conference is possible. The hotel has the capabilities to stream the presentation and they have organized such events in the past.

There follows a discussion when the videos of the accepted papers should be requested: after acceptance or just before the conference? It is agreed to do this before the conference. Everything is delayed except for the publishing of the papers. Preneel urges to make the guidelines on how to make the videos available as soon as possible.

**Decision 3** (unanimous)**.** *The Board approves to reschedule Eurocrypt 2021 to October 17 to 21 at the same location (Zagreb, Croatia).*

Boyd asks about any implications for *Eurocrypt 2022*. The President confirms that the assumption still is that this has no implication for the *Eurocrypt* conference in 2022.

2.3. **Crypto 2021.** Kolesnikov already mentioned the limitations: with the current rules from UCSB the auditorium and cafeteria are significant constraints. The President suggests to assume these restrictions still apply in August: would it be possible to hold a hybrid event? Halevi thinks that if these restrictions are still in place in August then people will not be able to travel and attend. If we can travel then there are probably fewer restrictions.

To the President it is not clear what the best option is to proceed. Kolesnikov thinks the current rules from UCSB do not allow for a physical event and it is unlikely to improve. He asks how to deal with sponsorship income. The Treasurer suggests to mention clearly that, if the event is digital, then the funds can be transferred to the next year.

The Board agrees to not make a decision about a physical or virtual *Crypto* 2021 yet.

2.4. **Discussion about other 2021 conferences.** Standaert mentions there are no significant updates for *CHES*. This is still planned to take place in China.

Yung states that *PKC* plans to follow *Eurocrypt* and go for a hybrid event if this is possible.

## 3. Topics

3.1. **Test-of-Time awards for old papers: update and discussion.** The President recalls the discussion about handing out Test-of-Time awards for older papers from the 1980s and 1990s. Handling all these older papers in one go seems not feasible. He asks the Board what to do with older *Asiacrypt* papers before it joined the IACR. The Board agrees that these papers should be considered.

The Board discusses how to best approach this. It is agreed that the regular test-of-time Committee is already under a lot of work and that a separate Committee should be created to investigate this.

> Action Point **1: President** *(no time set)*:
> Create a concrete proposal for the Test-of-Time awards for the 1980s and 1990s papers. Preneel and Abe will join this Committee.

3.2. **Discussion about sharing videos in Asia.** The President recalls that access to YouTube is difficult from China. How should we proceed to share the IACR videos in these regions? Yu has looked into this and suggests the Chinese video sharing platform Bilibili. McCurley has reservations about maintaining two video hosting platforms for the IACR: should we host this ourselves? Yu will try and get more information from Bilibili if this fits IACR's requirements (sharing hundreds of videos after a conference took place).

Action Point **2: Yu** *(no time set)*:
Look into the Bilibili video sharing platform and present a proposal if this fits the IACR's needs.

3.3. **New journal proposal update.** After the last Board meeting the New Journal Committee did not meet: this is planned for next Monday. Bos explains they come in Q1 with a concrete proposal before the Board.

## 4. Closing Matters

Abdalla closes the meeting at 00h00 CEST.