MINUTES IACR BOARD MEETING *VIRTUAL-3 '21*

17 MARCH 2021

1. OPENING MATTERS

1.1. **Welcome, roll of attendees, identification of proxies.** At 16h03 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 no-one holding proxies. These minutes are reordered to the original agenda for consistency.

Heninger is present for the first half of the meeting, during her absence LaMacchia has her proxy. Lepoint is present for the first half of the meeting, during his absence Stebila has his proxy.

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); Nadia Heninger (Director 2019-2021). 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);

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)); Vincent Rijmen (Journal of Cryptology Editor-in-Chief 2021–2023). Douglas Stebila (Membership Secretary (2017-2022)); Bo-Yin Yang (*Asiacrypt'22* General Chair (2021-2022)).

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

Absentees (Elected). Moti Yung (Director 2021-2023, *PKC* 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-2 '21.*

2. CONFERENCES

2.1. **PKC 2022 Proposal.** The President goes over the proposal for *PKC'22* in Yokohama, Japan. Lepoint asks if the possibility for a hybrid event has been taken into account. LaMacchia confirms this has been incorporated in the budget sheet. Baldimtsi wonders if and by how much the fee will differ by attending in person or virtually. The President explains that this will be determined when the situation arises.

Decision 2 (unanimous). *The Board approves the proposal for PKC'22 in Yokohama, Japan selected by the PKC Steering Committee with Program Chair Goichiro Hanaoka and General Co-Chairs Junji Shikata and Yohei Watanabe.*

2.2. **Update on 2021 conferences.** Kolesnikov announces that *Crypto'21* will be a virtual event. The UCSB will not host any external events on campus this summer. Just as previous virtual events there will be no registration fee although attendants should pay for their IACR membership fee. Kolesnikov asks what to do if we receive more sponsorship income than we can spent in a virtual setting and if we should set different levels to make the choice easier for the sponsors. LaMacchia explains that the guidelines are clear that the General-Chair is free how to collect and spent the sponsorship income. After a discussion it is decided to go for different levels of sponsorship as the guideline. McCurley suggests to update the website soon to make it clear that *Crypto* will be a virtual event.

Schwabe gives an update with respect to *CHES*. It was decided to postpone the physical event by one year. There is no financial impact since no contract was signed with the venue. The General Co-Chairs will remain the same and it is planned to be held in Beijing, China. McCurley recalls that it was hard to organize the requested virtual booths for the sponsors. If we want this again this year we should not wait until the last minute. The President agrees we should start this in-time.

Batina explains that there is still hope for a hybrid *Eurocrypt'21*. The final decision to go virtual or hybrid is postponed until July.

3. APPOINTMENTS, COMMITTEES, AND POLICIES

3.1. ***Eurocrypt 2023* program co-chair appointment (one name).** The President recalls the Board needs to select the second Program Co-Chair for *Eurocrypt 2023*. The first Program Co-Chair is Carmit Hazay. Several excellent candidates are nominated, and after discussion a candidate is selected.

Decision 3. *Martijn Stam is appointed Program Co-Chair for Eurocrypt 2023. [Stam subsequently accepted.]*

4. TOPICS

4.1. **New journal proposal update.** Bos shared the proposal for the New Journal before the Board Meeting with the Board. He goes over the various options and questions outlined in the document. There is a discussion around the name of the journal which is currently referred to "Annals of Cryptology" in the proposal. It is indicated that the usage of "Annals" is not preferred, the use of "of the IACR" in alternative title suggestions does not indicate clearly what the journal is about and might conflict with the inclusion of some of the events at the border of the IACR as special issues (such as Latin-, Africa- and Indo-crypt). Suggestions made where "Transactions on Cryptology" and "Communications in Cryptology" among others. Bos indicates that choosing the name is a low-priority task but it is good to keep this discussion ongoing.

The suggested 300 submitted papers per year (and the corresponding 75 board members) is considered to be conservative and might grow much larger very fast. There is a suggestion to have additional "junior board members" to increase the total number of Board Members for this new journal.

There is a discussion related to the cost of the new journal. Possible ways to pay for the new journal expenses are to allow for advertisement in the new journal, increase conference fees or reserve a separate line-item globally. This will be discussed in more detail once we have a better understanding of the approximate cost of the new journal.

Decision 4 (unanimous)**.** *The Board approves with the stated overall goals and scope of the new journal proposal and allows the New Journal Committee to reach out to different parties to get quotes for reviewing software and publishing services.*

5. CLOSING MATTERS

Abdalla closes the meeting at 18h06 CEST.