MINUTES IACR BOARD MEETING *VIRTUAL-12 '21*

15 DECEMBER 2021

1. OPENING MATTERS

1.1. **Welcome, roll of attendees, identification of proxies.** At 22h05 CET 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 Abe holding proxy for Guo, Stebila for LaMacchia and Lepoint, Preneel for Rijmen and Halevi for Kolesnikov. These minutes are reordered to the original agenda for consistency.

1.1.1. *Roll of Attendees.*

Attendees (Elected). Michel Abdalla (President 2020-2022); Joppe Bos (Secretary 2020-2022); Shai Halevi (Vice President 2020-2022, *TCC* Steering Committee); Masayuki Abe (Director 2021-2023); Nadia Heninger (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); Douglas Stebila (Membership Secretary (2017-2022)); Bo-Yin Yang (*Asiacrypt'22* General Chair (2021-2022)).

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

Absentees (Elected). Brian LaMacchia (Treasurer 2020-2022); Marc Fischlin (Director 2020-2021); Tancrède Lepoint (Director 2021-2023); Anna Lysyanskaya (Director 2019-2021).

Absentees (Appointed). Jian Guo (*Asiacrypt'21* General Chair (2020-2021)); Vincent Rijmen (Journal of Cryptology Editor-in-Chief 2021–2023); Vladimir Kolesnikov (*Crypto'21* General Chair (2020-2021)).

Absentees (Representatives and Others). 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-11 '21.*

2. CONFERENCES

2.1. *RWC* **2022 Update.** Schwabe recalls that RWC decided, following the latest updates from the Dutch authorities, to postpone the event to April 13-15 2022. The RWC Steering Committee has made this decision after a discussion with the venue. A mail has already been sent to inform speakers and participants. The President agrees that it is reasonable to postpone *RWC*. Schwabe thanks Stebila for the all the help with the registration system.

2.2. **Update on other upcoming conferences.** Yung reports that the local organization of *PKC* has expressed their desire to hold the event virtual. The PKC Steering Committee agrees with the recommendation. The President asks the Board if there are any concerns with going virtual and no-one objects.

Preneel reports no updates for *FSE*. He hopes the situation will improve and that a hybrid event will be possible. Boyd recalls that the current situation in Norway does not look good for *Eurocrypt*. The decision what to do is postponed to next year.

3. Topics

3.1. **Women's networking reception at *Crypto* 2022.** Orman explains she wants to organize a networking reception for women at *Crypto* 2022 based on the success of the women's cryptography panel at *Crypto* 2021. There is funding money available for such an event. She asks the Board if they are willing to support such a proposal. The Board agrees but sees this as a decision of the General Chair. Bishop fully supports this proposal and will contact Orman to plan this event. McCurley wonders how to organize this if *Crypto* is a hybrid event: what about the virtual attendance? The President appreciates this initiative to improve our diversity. We have had too much on our plate due to COVID.

3.2. **Update on the new journal proposal.** Bos explain that the New Journal Committee met with Cambridge University Press to discuss the options and possibilities to host the papers through their system. CUP would try and come back with a detailed offer before this Board meeting including options to support long term digital preservation archive services. Unfortunately we did not rceive any update yet.

Schwabe mentions the New Journal proposal has been presented to the CHES Steering Committee. TCHES does not see this as a threat to the Transaction. There might be some competition but this is not perceived as a significant concern. McCurley warns that one of the risks with the New Journal is that the IACR might stretch itself too thin. We only have a small number of volunteers. Bos suggests we try to recruit more volunteers but we need to be more specific what skills we look for and what tasks we have available. Stebila recalls that the Transactions are not indexed by Web of Science: this seems like a problem for this New Journal as well. Bos explains that the New Journal might help here since it solves too many self-citations from the Transactions.

3.3. **Other topics.** The President sees some potential problems when *PKC*, *FSE* and *RWC* all will take place in the same month. How can we handle this for the virtual parts? We need a way that the General Chair can appoint people to run the virtual part of the conference. Halevi agrees and asks if we can train local people for this task. McCurley explains that this is possible now we have more experience. Bishop volunteers to be trained to see if this is indeed realistic and then someone local can do this for *Crypto* 2022. McCurley agrees that this makes sense. It should be noted that the regular cases can be covered by a training. Exceptional cases such as interlopers during the meeting or technical issues (not being to share screen due to strange OS settings) are more difficult.

4. Closing Matters

The President thanks Heninger and Fischlin for their work on the Board. Abdalla closes the meeting at 22h55 CET.