MINUTES IACR BOARD MEETING *VIRTUAL-6 ’22*

21 JUNE 2022

1. OPENING MATTERS

1.1. **Welcome, roll of attendees, identification of proxies.** At 16h23 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 the following proxies: Stebila holds Bos’s proxy; Lepoint holds Baldimtsi’s proxy and Bos’s proxy when Stebila leaves; Yang holds Schwabe’s proxy; Yung holds Standaert’s proxy when absent; Preneel holds Rijmen’s proxy; Guo holds Zhang’s 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); Masayuki Abe (Director 2021-2023); Tancrède Lepoint (Director 2021-2023); Jian Guo (Director 2022-2024); Anna Lysyanskaya (Director 2022-2024); Bart Preneel (Director 2020-2022, *FSE* Steering Committee); Bo-Yin Yang (Director 2022-2024, *Asiacrypt’22* General Chair); Moti Yung (Director 2021-2023, *PKC* Steering Committee);

Attendees (Appointed). Allison Bishop (*Crypto’22* General Chair (2021-2022)); Colin Boyd (*Eurocrypt’22* General Chair previously *Eurocrypt’21* General Chair (2020-2022)); Britta Hale (*Crypto’23* General Chair (2022-2023)); Douglas Stebila (Membership Secretary (2017-2022)); Damien Stehlé (*Eurocrypt’23* General Chair (2022-2023));

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

Absentees (Elected). Joppe Bos (Secretary 2020-2022); Peter Schwabe (Director 2020-2022); Francois-Xavier Standaert (Director 2020-2022, *CHES* Steering Committee);

Absentees (Appointed). Foteini Baldimtsi (Communications Secretary (2019-2022)); Vincent Rijmen (Journal of Cryptology Editor-in-Chief 2021–2023); Fangguo Zhang (*Asiacrypt’23* General Chair);

Absentees (Representatives and Others). Hilarie Orman (Archivist); Tal Rabin (Code-of-conduct Liaison); Kenny Paterson (*RWC* Steering Committee); Yu Yu (Webmaster).

1.2. **Review and approve agenda.** Yang suggests deferring the appointment of the 2nd Crypto 2024 program co-chair since it was not known in advance that multiple appointments would be taking. It is further pointed out that the second co-chair is often taken to complement the profile of the first co-chair, so the second appointment cannot be made until the first has had a chance to accept. It is agreed to defer.

1.3. **Approve minutes from last BoD virtual meeting.** The Vice-President thanks the Secretary for the completion of the minutes which have been shared before the current Board Meeting. Halevi calls for a vote to approve the minutes.

Decision 1. *The Board approves the Minutes of the IACR Board Meeting Virtual-5 ’22.*

2. CONFERENCES

2.1. **Update on 2022 conferences.** Boyd provides a review of *Eurocrypt 2022*. In-person attendance was over 400. Hybrid operations proceeded well. Boyd will be working with the Treasurer to finalize the financial books. Boyd received notification of 16 Covid cases from conference attendees. Abdalla thanks Boyd for successful event on behalf of the Board.

Bishop provides an update on *Crypto 2022*. Registration is open. Bishop asks members to help widely circulate the announcement about student stipends. Bishop notes the UCSB shuttle service from the airport will not be running this year due to staff shortages. LaMacchia suggests looking into charter service on Sunday.

There are no updates for *CHES* or *TCC*.

Yang provides an update on *Asiacrypt 2022*. Reservations are on track, but deferring deposits as long as possible.

2.2. **Update on 2023 conferences.** LaMacchia confirms *RWC 2023* is on track for Tokyo in March.

Stehlé notes that he is negotiating the contract with the venue for *Eurocrypt 2023* with a deposit expected for September.

3. Appointments, committees, and policies

3.1. **Crypto'24 program co-chair appointment.** The President recalls the Board needs to select the Program Co-Chair for *Crypto 2024*. The second Program Co-Chair for *Crypto 2024* will be decided at the next board virtual meeting. Several excellent candidates are nominated, and after discussion a candidate is selected.

Decision 2. *Douglas Stebila is appointed Program Co-Chair for Crypto 2024. [Stebila subsequently accepted.]*

3.2. **New journal editor-in-chief appointments.** The President recalls the suggestion from the new journal committee that the editor-in-chief appointments be designed to stagger with appointments every 2 year, which would lead to one initial 2-year appointment and one initial 4-year appointment.

Preneel reports feedback from the FSE and CHES steering committees, which continue to have concerns about overlap between the new journal and these venues.

Preneel suggests that appointing an EiC before resolving these concerns could send the wrong message; and appointing an EiC before a membership vote could be problematic if the name leaks. Yung suggests further reflection is merited as well. Lysyanskaya believes it is okay to select an EiC before finalizing the journal parameters to have an EiC available to help steer the process. McCurley notes his increasing discomfort with the new journal proposal around details of the acceptance criteria. Stebila notes concerns from the Selected Areas in Cryptography (SAC) Steering Committee that the new journal will likely impact submissions to conferences like SAC, for which there is not a clear resolution (although it may be inherently unresolvable). Abdalla comments that there are many concerns that still need to be addressed and that moving ahead with selection of an EiC may be better to hold off on until the position is more well-established. Yung acknowledges that many of the issues noted above have been heard but not fully addressed by the committee, but the committee wants to ensure the new journal would enhance the situation for both IACR and non-IACR venues, by building in a lot of flexibility. Lepoint comments that in order to make progress at the Board we should have a clear enumeration of concerns and responses. Halevi comments that having the Board and the new journal committee both designing the new journal will lead to a bad outcome: either an EiC should be appointed to push the process, or the new journal committee should submit a full proposal for an up-down vote by the Board.

Abdalla wants to find out from the Board on how it wants to proceed with voting. Yung suggests that a clear timeline from the Board to the journal committee would be helpful. Stebila echoes Lepoint's suggestion on a clear enumeration of concerns and responses, and further suggests that the Board should expect to receive a detailed proposal from the new journal committee, with statements of scope, acceptance criteria, operations, finances, etc., for a Board vote of approval before appointing an EiC. Lysyanskaya suggests that having an EiC who can drive this forward with a clear vision would be helpful. Yang believes that having an EiC before a clear vision will exasperate the competing interests, rather than help. Yang also agrees that a detailed proposal should be expected.

Decision 3. *The Board approves a motion to postpone the selection of an EiC until after receiving a more detailed proposal from the new journal committee.*

Decision 4. *The Board approves a motion requesting the new journal committee submit a detailed proposal by August 7.*

4. Closing Matters

Abdalla closes the meeting officially at 18h13 CEST.