MINUTES IACR BOARD MEETING *VIRTUAL-2 '22*

17 FEBRUARY 2022

1. Opening Matters

1.1. **Welcome, roll of attendees, identification of proxies.** At 22h03 CET Halevi opens the meeting and briefly goes around for an introductory round, confirming attendees and establishing who is holding proxies. There are 19 full time attendees with Preneel holding proxy for Rijmen and Bishop for Lysyanskaya after she leaves (at 23h07 CET). Malkin joins at 22h08 CET, McCurley at 22h13 CET and Lepoint at 22h22 CET. 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); Brian LaMacchia (Treasurer 2020-2022); Masayuki Abe (Director 2021-2023); Jian Guo (Director 2022-2024); Bart Preneel (Director 2020-2022, *FSE* Steering Committee); Tancrède Lepoint (Director 2021-2023); Anna Lysyanskaya (Director 2022-2024); Peter Schwabe (Director 2020-2022); Francois-Xavier Standaert (Director 2020-2022, *CHES* Steering Committee); Bo-Yin Yang (Director 2022-2024, *Asiacrypt'22* General Chair (2021-2022)); Moti Yung (Director 2021-2023, *PKC* Steering Committee).

Attendees (Appointed). Allison Bishop (*Crypto'22* General Chair (2021-2022)); Colin Boyd (*Eurocrypt'22* General Chair); Britta Hale (*Crypto'23* General Chair (2022-2023)); Douglas Stebila (Membership Secretary (2017-2022)); Fangguo Zhang (*Asiacrypt'23* General Chair (2022-2023)).

Attendees (Representatives and Others). Tal Malkin (*TCC* Steering Committee); Kevin S. McCurley (Database Administrator).

Absentees (Appointed). Foteini Baldimtsi (Communications Secretary (2019-2022)); Mitsuru Matsui (*Asiacrypt* Steering Committee); Kenny Paterson (*RWC* Steering Committee); Vincent Rijmen (Journal of Cryptology Editor-in-Chief 2021–2023).

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 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 (unanimous)**.** *The Board approves the Minutes of the IACR Board Meeting Virtual-1 '22.*

2. Conferences

2.1. **Update on upcoming conferences.** Yung report that *PKC* will be held completely virtual from March 8-11. The realization of this virtual event is ongoing with McCurley. Preneel explains that *FSE* will be held as a hybrid event in Athens, Greece on 20-25 March 2022. The registration just opened. Schwabe reports that *RWC* will also be organized as a hybrid event on April 13-15, 2022 in Amsterdam, the Netherlands. The registration just opened and they already had a meeting with the venue. Boyd recalls that *Eurocrypt* will take place as a hybrid event in Trondheim, Norway on May 30 to June 3, 2022. The affiliated workshop program has been finalized and the sponsorship is looking good. Boyd had a meeting with an accountant to investigate if we need to pay tax on our sponsorship income. There follows a discussion around this topic and it is mentioned that in the past we ensured that sponsorship is done directly to the IACR in the USA. This will be followed up to ensure we follow the proper procedures. Bishop reports that everything for *Crypto* is looking good. The contract with UCSB has been signed and the submission server is up. Schwabe reports that the recent location change for *CHES* is already on the website but that more information needs to be added and updated. Malkin reports that *TCC* will take place in Chicago, USA on November 7-10 2022. Nothing special to report.

2.2. **Eurocrypt 2023 Search.** The President summarizes that the search for the location of *Eurocrypt* is still ongoing. Multiple options have been explored without concrete success. Preneel and Schwabe report to have asked around and will report back this week. Various potential options and locations are discussed.

3. TOPICS

3.1. **IACR CoI policy clarification.** Schwabe brings a question to the Board about our Conflict-of-Interest policy. This states that one has an automatic COI with an author "if one is or was the thesis advisor to the other, no matter how long ago". The question if this thesis advisor means PhD thesis advisor only or if this also applies to Bachelor or Master thesis advisors. It becomes clear that different members of the Board interpret this differently and there is consensus this needs to be clarified. Everyone agrees that this should include the PhD thesis advisor but other thesis advisors might be included depending on the involvement. It is agreed that the text in the CoI needs to be adjusted. Stebila volunteers to update the text.

> Action Point **1: Stebila** *(no time set)*:
> Update the CoI text with respect to the thesis advisor and present for approval to the Board.

3.2. **New journal proposal update and vote.** Bos provides a summary of the New Journal Committee. This summary was communicated to the Board over e-mail with the recommendations of the New Journal Committee which they propose to vote on.

Preneel thanks the Committee for the excellent work. He reports that there was a discussion about the New Journal in the *FSE* Steering Committee earlier this same day. The *FSE* SC believes such a new journal will make the publication landscape too complex, fear this might lead to more reviews overall and make it harder to find good reviewers for the Program Committees. They suggest to move all IACR publications to the Transaction model. Preneel also report on discussions he has had with the *CHES* Steering Committee: they are indifferent and see no impact for the Transactions on Cryptographic Hardware and Embedded Systems (TCHES).

Yung recalls that these fears have been discussed in-depth in the Committee. The Journal should be viewed as an alternative: not a replacement. It is not up to the SC of one area conference to dictate what the other area conferences should do in terms of publication model. However, we need to know if there is a negative impact due to the creation of this new journal on one or more of our area conferences. Stebila points out that we have much more areas in cryptology than just the four area conferences.

Halevi is in favor to move forward with the new journal and try it out: this is something proposed by the community. The President believes there is room in our community for this new journal. He sees the clear advantages of the new publication outlet but understands the concerns by the *FSE* SC. He suggests to eventually present the full proposal to our membership and asks for approval in a referendum to the members.

Decision 2. *The Board agrees in principle to the creating of the New Journal where*

- *HotCRP is used for the submission and review step just as we do for the Transactions.*
- *The editing step is handled similar to how the Transactions handle this currently and then work towards automating this.*
- *The hosting step is performed by ourselves and build on top of the rework done for the ePrint archive.*
- *The Board appoints the Editors in Chief withing the next two months.*

4. CLOSING MATTERS

Halevi closes the meeting at 23h35 CET.