MINUTES IACR BOARD MEETING *VIRTUAL-5 '22*

25 MAY 2022

1. Opening Matters

1.1. **Welcome, roll of attendees, identification of proxies.** At 16h02 CEST the President 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 LaMacchia holding proxy for Stebila (when not present), Yung holding proxy for Standaert and Rijmen holding proxy for Preneel. Stebila joins 16h15 and Rijmen joins 16h25. 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); Tancrède Lepoint (Director 2021-2023); Anna Lysyanskaya (Director 2022-2024); Peter Schwabe (Director 2020-2022); Bo-Yin Yang (Director 2022-2024, *Asiacrypt'22* General Chair (2021-2022)); Moti Yung (Director 2021-2023, *PKC* Steering Committee).

Attendees (Appointed). Foteini Baldimtsi (Communications Secretary (2019-2022)); Allison Bishop (*Crypto'22* General Chair (2021-2022)); Colin Boyd (*Eurocrypt'22* General Chair (2021-2022)); Britta Hale (*Crypto'23* General Chair (2022-2023)); Vincent Rijmen (Journal of Cryptology Editor-in-Chief 2021–2023). Douglas Stebila (Membership Secretary (2017-2022)); Damien Stehlé (*Eurocrypt'23* General Chair (2022-2023)); Fangguo Zhang (*Asiacrypt'23* General Chair (2022-2023)).

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

Absentees (Elected). Bart Preneel (Director 2020-2022, *FSE* Steering Committee); Francois-Xavier Standaert (Director 2020-2022, *CHES* Steering Committee).

Absentees (Representatives and Others). Mitsuru Matsui (*Asiacrypt* Steering Committee); 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. Michel calls for a vote to approve the minutes.

Decision 1 (unanimous)**.** *The Board approves the Minutes of the IACR Board Meeting Virtual-4 '22.*

2. Conferences

2.1. **Update on upcoming conferences.** Boyd gives an update on *Eurocrypt*, everything is going as planned and there are currently around 420 in-person registrations. Next, Bishop asks if the computer labs are needed for *Crypto*? Most people will bring their own laptops and the wireless internet is very good at the campus. It is agreed that this is not needed. She asks if we need plan for a Board meeting. The President suggests we hold a hybrid Board meeting and plan for a longer meeting in case we need the time. The Treasurer suggests to use this longer meeting to have a discussion about the long-term strategy for the IACR. The Board agrees that a hybrid Board of Directors meeting makes sense followed by a separate discussion on the long-term IACR strategy. Bishop continues to explain that an increased number of papers have been accepted but that the length of the presentations remains the same as last year. This means that the conference will start each day earlier and that one afternoon session has been added. Following the examples at *RWC'22* and *Eurocrypt'22* she is investigating options to provide childcare. This seems not straight-forward: UCSB is not willing to assist due to liability issues. The plan is to recommend local childcare providers and help with any childcare related questions.

Malkin explains that the venue for *TCC'22* cannot commit yet and that they are working on alternative options. Yang explains that *Asiacrypt'22* is on track. Guo asks if we expect Taiwan to open up for intercontinental travel. This is indeed the expectation by Yang. Paterson recalls that *RWC'23* will be held in Tokyo, Japan in March 2023. Kazue Sako will be the local organizer and is part of the Steering Committee. The President asks if this clashes

with any of our other conferences. This is not the case and Yung reminds the Board that *PKC* takes place in mid-May.

2.2. **PKC 2023 conference proposal.** Yung presents the proposal for *PKC* 2023 in Atlanta, Georgia which has been shared with the Board before the meeting. The proposed Program Chairs are Sasha Boldyreva and Vladimir Kolesnikov. The proposed General Chairs are Daniel Genkin and Joseph Jaeger. The Treasurer remarks that the budgetted USD 15k sponsorship income seems too optimistic.

Decision 2 (unanimous)**.** *The Board approves the recommendation from the PKC Steering Committee to hold PKC 2023 in Atlanta, Georgia with Boldyreva and Kolesnikov as Program Chairs and Genkin and Jaeger as General Chairs.*

3. Topics

3.1. ***Eurocrypt* 2024 Program Co-Chair Appointment.** The President recalls that we need to appoint a second Program Co-Chair for *Eurocrypt 2024* who serves with Joye. Before the Board meeting several excellent candidates have been nominated, and after discussion a candidate is selected.

Decision 3. *Gregor Leander is appointed Program Co-Chair for Eurocrypt 2024. [Leander subsequently accepted.]*

3.2. **New license requirement for ePrint.** McCurley explains the potential need for a dedicated IACR license for the Cryptology ePrint Archive. This proposal of the license is as follows:

IACR perpetual, non-exclusive license The URI `https://iacr.org/license/1.0/` is used to record the fact that the submitter has granted the following license to IACR on submission of an article:

- I grant IACR a perpetual, non-exclusive license to distribute this article.
- I certify that I have the right to grant this license.
- I understand that submissions cannot be completely removed once accepted.
- I understand that IACR reserves the right to reclassify or reject any submission.

He suggests that if we decide to adopt this then the IACR license should be the default. Halevi suggests to have a mechanism to add more license options in the future and a link to contact the editors with questions. Lepoint is not in favor with this last suggestion: it is not our job to help with the selection of the appropriate license: Halevi agrees.

Decision 4. *The Board decides to adopt the IACR perpetual, non-exclusive license and make this the default license for the Cryptology ePrint Archive.*

3.3. **Revised conflict of interest policy.** Stebila shows the update to the Conflict of Interest policy based on the discussion and feedback from the last Board meeting.

Decision 5 (unanimous)**.** *The Board approves the updated Conflict of Interest text which clarifies the role of undergraduate theses.*

3.4. **New journal proposal Editor-in-Chief Role Definition.** Bos recalls that the Board decided in the February Board meeting to select the Editor-in-Chief(s) for the new journal within two months and that we are already late. The President asks if the new journal committee has a recommendation about the number of EiC. Bos summarizes the discussion from the new journal and there is consensus in the committee to select two EiCs.

Decision 6. *The Board decides that the new IACR journal will have two Editor-in-Chiefs.*

Multiple options for the duration of this EiC position ar discussed. Options include one year just as for the Transactions or serving three years. There is concern that doing this for multiple years would require a significant amount of time but the plan is to offload some of this work to the area chairs. Yung also recalls that the first EiCs will probably have probably more work to set the standard compared to the future EiCs. The President asks Bos if he can align with the new journal committee about the time these EiC will serve. If we know this soon then the Board can move forward.

3.5. **Childcare at IACR conferences.** Schwabe gives an overview of the childcare facilities we offered over the years. This started at *CHES* 2018 where a breast feeding room was offered but not used. At *RWC* 2022 they organized a nanny and received very positive feedback. It might be good to add a separate section about this in the General Chair guidelines document.

Rijmen mentions that we should be careful. People from different cultures have different expectations what a nanny should or should not do. Malkin wonders if we should align with local childcare providers. Boyd explains that for *Eurocrypt* 2022 childcare was explicitly advertised on the webpage. Request for help was being forwarded

to local childcare services since the conference venue had not received any such requests before and was not able to assist. Lysyanskaya agrees that offering such simple support is often already very helpful.

4. Closing Matters

The President closes the meeting at 18h07 CEST.