MINUTES IACR BOARD MEETING *VIRTUAL-5 '21*

20 MAY 2021

1. Opening Matters

1.1. **Welcome, roll of attendees, identification of proxies.** At 22h02 CEST Abdalla opens the meeting and briefly goes around for an introductory round, confirming attendees and establishing who is holding proxies. There are 18 full time attendees with Lepoint holding proxy for Halevi, Heninger for Lysyanskaya and Bishop (when not present) and Abe for Guo. Batina leaves at 23h30 and Schwabe has her proxy. These minutes are reordered to the original agenda for consistency.

1.1.1. *Roll of Attendees.*

Attendees (Elected). Michel Abdalla (President 2020-2022); 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); 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 previously *Eurocrypt'21* General Chair (2020-2022)); Vladimir Kolesnikov (*Crypto'21* General Chair (2020-2021)); 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). Shai Halevi (Vice President 2020-2022, *TCC* Steering Committee); 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).

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-4 '21.*

2. Conferences

2.1. **Asiacrypt 2023 Proposal.** Zhang presents the proposal for *Asiacrypt* 2023 in Guangzhou, China to the Board. The President thanks Zhang to consider the hybrid option as well in the proposal. LaMacchia thinks that the estimated 425 attendees is exceptionally high for Asiacrypt but this should not be a problem for the budget: we can make a loss. Stebila asks about the streaming possibilities outside China. Yung recalls that this worked reasonably well last time but could be improved. Preneel wonders if the Chinese students can effort this registration fee. Zhang mentions that last time the CACR supported local students. The President thanks Zhang and will make sure the Board votes on this over e-mail soon.

Action Point **1: President** *(no time set)*: Arrange voting over e-mail for the Asiacrypt 2023 proposal.

2.2. **Eurocrypt 2021 report.** Standaert provides a summary of the Eurocrypt report which has been shared with the Board before the Board meeting. Some of the main points are the workload for the Program Committees members (over 20 papers per reviewer) and rejections for subjective reasons. This latter point is a good case for the New Journal. Stebila notices that there were only a couple contributions from our *CHES* community. We need to investigate how this can be mitigated. Moreover, reviewing over 20 papers per PC member seems too much: this should be fixed.

McCurley asks if the automatic review assignment worked well. Standaert explains the process, it worked well but required still some manual checking. Assigning discussion leaders for papers early one was a very good idea.

There follows a discussion where and if to post this document online. The ePrint archive is not the best venue and it is agreed that this could be hosted on the IACR page.

2.3. **Update on 2021 conferences.** During *PKC* there was again a problem with Springer. The participants had no access to the proceedings, this is already the second time this happened. Overall 300 people attended the conference. The organization of *Crypto* is going according to plan. The conference will be fully virtual. The sponsorship opportunities with preset levels seem to be working much better. The *CHES* conference takes place virtually. Not much has been arranged and the Board will reach out to the organizers soon. The *Eurocrypt* conference will still possibly be a hybrid event. More details will be discussed in a separate call tomorrow. Batina explains that they are discussing parallel tracks or shorter presentations. There are many things to consider for a hybrid event: how to exactly organize the physical presence etc. This is all on-going and she will update the Board in the upcoming Board meetings. There are no updates from *TCC* nor *Asiacrypt*.

3. Appointments, committees, and policies

3.1. **2021 Election committee.** The President explains we need to start to organize the Election Committee. We are looking for 3 directors and the President asks for volunteers. Both Lepoint and Abe volunteer.

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

Decision 2. *Helena Handschuh is appointed Program Co-Chair for Crypto 2023. [Handschuh subsequently accepted.]*

4. Topics

4.1. **New journal proposal update.** Bos provides an update on the progress of the New Journal committee. Bos and Nigel have been in contact with EasyChair. They did not seem eager to talk to us but did provide us with an instance we could experiment with and look what features they had.

Bos and Nigel spoke with a team from Cambridge University Press. They demonstrated the Open Engage platform (see: `https://www.cambridge.org/engage/coe/public-dashboard`). This is currently a pre-print service (like ePrint but it assigns DOIs) which is completely open for users. CUP are already planning to add journal features for a number of chemistry journals. They showed us their reviewing back-end: it did miss some important features on our requirement list. These missing features could be integrated at a cost, the time-frame was not clear.

Bos and Schwabe had a meeting with Radboud Publishing. This is a new (per April 1st this year) non-profit publishing house. They do the reviewing based on OJS and publish in-house. They do not ask any publishing fee; only if you have a grants which foresees for open access publishing they will accept this money. They were quite surprised about our potential volume of papers and it is likely that any future quote might ask a per paper contribution. They are already in contact with developers of OJS to add features and they will invite for a call with us, OJS and them. This call is scheduled for later this week. The risk is that they are very new and the timeline to adjust OJS is unclear.

Bos and Schwabe had a meeting with RUB where we are currently hosting our Transactions. The team of the university we met consists of a number librarians who are in charge to put the final version pdfs online, assign DOIs etc. They do not perform any post-processing, this is done by the labs responsible for the Transactions at the university (which is an approach that does not scale well). Integration in a reviewing system is far outside their comfort zone: so the solution with Bochum would (probably) look like hotcrp + hosting. Schwabe, McCurley, and Bos will follow-up in a two-stage approach, first with the teams behind the Transactions and then the librarians.

The President thanks Bos for leading this effort.

5. Closing Matters

Abdalla closes the meeting at 00h10 CEST.