MINUTES IACR BOARD MEETING *VIRTUAL-9 '21*

22 SEPTEMBER 2021

1. Opening Matters

1.1. **Welcome, roll of attendees, identification of proxies.** At 16h06 CEST Halevi opens the meeting and briefly goes around for an introductory round, confirming attendees and establishing who is holding proxies. There are 22 full time attendees with Preneel holding Rijmen's proxy, Schwabe holding proxing for Batina, LaMacchia holding Heninger's proxy, Abe holding Lepoint's proxy, Lysyanskaya holding Bishop's proxy, Shai holding Lysyanskaya's proxy (all proxies are valid when the person is not present due to people joining later or leaving earlier). 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); Brian LaMacchia (Treasurer 2020-2022); Masayuki Abe (Director 2021-2023); Marc Fischlin (Director 2020-2021); Nadia Heninger (Director 2019-2021); Anna Lysyanskaya (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).

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); Jian Guo (*Asiacrypt'21* General Chair (2020-2021)); Vladimir Kolesnikov (*Crypto'21* General Chair (2020-2021)); Douglas Stebila (Membership Secretary (2017-2022)); Bo-Yin Yang (*Asiacrypt'22* General Chair (2021-2022)); Moti Yung (Director 2021-2023, *PKC* Steering Committee).

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

Absentees (Elected). Tancrède Lepoint (Director 2021-2023).

Absentees (Appointed). 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 joins the Board Meeting approximately half an hour late. 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-8 '21.*

2. Conferences

Abe provides a short update on the Election status. So far one nomination has been received and the deadline is the end of this month (September). However, he is confident that sufficiently many candidates will be nominated.

2.1. **Update on remaining 2021 conferences.** Kolesnikov provides an update with respect to *Crypto'21*. He is in the process of purchasing t-shirts with the Crypto 2021 logo for some people who helped with the conference and wants to check the cost with the Board. There are no objections against this cost which has been included in the budget.

Batina gives an update on *Eurocrypt'21*. At the moment there have been over 150 in-person registrations and over 200 virtual registrations. Standaert asks about the number of speakers on-site and the total number of speakers attending in-person is not known yet.

Guo explains that *Asiacrypt'21* decided to go completely virtual. Stebila suggests to align on the registration and sponsorship.

Halevi report there is no significant update with respect to *TCC*. The plan is to have an in-person or hybrid event mid-November in Raleigh, USA similar to *Eurocrypt*.

There is no update from *RWC*; the Steeing Committee will meet next week.

3. TOPICS

3.1. **New journal update.** Bos presents the work the New Journal Committee have been working on. The slides have been shared with the Board over e-mail and in the repository before the Board Meeting. The suggestion to create a new IACR journal was suggested by a number of members from the community. Some of the main goals of this new journal include the following.

- Diamond or Gold Open Access publishing model.
- Fast and consistent turnaround time (decision in 3 months).
- Allow for scaling to handle the current (and future) size of the field.
- Respect all areas of the community (theory/applied/practice, symmetric/public key/protocols/implementation, geographic area).
- Reduce overall reviewing load for our community.
- Allow another outlet for our community to publish without the need to travel to conferences.

Bos summarizes the conversations and outcomes with Ruhr University Bochum, Radboud Publishing, Cambridge University Press, and EasyChair. The work-flow of the New Journal has been divided into three steps

Step 1. Submission and review system
Step 2. Editorial management system
Step 3. Hosting system

The final recommendation of the New Journal discussion is to use the HotCRP conference management software just as the Transaction use already (Step 1). Perform the post-processing ourselves by hiring someone to do this work (Step 2) and host and publish ourselves (Step 3). This has the benefit to reduce cost as much as possible but has as a risk that we increase the permanent work for the IACR. An estimate for the various costs and effort is given in the presentation.

There is a discussion about the various aspects of the journal including how to pay for this. Bos explains that the technical decisions how to run the Journal are up to the Editorial Board while the Board of Directors need to decide how we will pay for this Journal after the Board has agreed that we want to move forward with this new journal. Preneel suggests we align with the Transaction to have a common answer how the New Journal and the Transactions compare and what their main differences are.

Decision 2 (unanimous)**.** *The Board agrees with the general recommendations of the New Journal Committee but asks to explore other options for Step 3 (such as CUP) and asks the New Journal Committee to propose a more concrete proposal before the end of the year including a more detailed cost analysis.*

3.2. **IACR school proposal.** Lepoint explains that we received one school proposal after two deadlines with no proposals. The School Committee recommends to fund the proposal for the requested amount of 10k euro under the condition that they increase the diversity of the invited speakers. Preneel thinks this is an excellent idea but suggests that we urge the organizers to fix a date if the school plans to take place this year.

Decision 3 (unanimous)**.** *The Board decides to follow the recommendation of the Schools Committee and fund the School on Combinatorial Techniques in Cryptography at TU Darmstadt, Germany.*

3.3. **Sponsorship of of RSA conference award.** Yung summarizes the proposal on behalf of Rivest and the CT-RSA Steering Committee if the IACR wants to become a co-sponsor for the "RSA Award for Excellence in Mathematics". The concrete proposal was shared with the Board before the meeting. The idea is that the award will get a sub-title "The Award is co-sponsored by the International Association for Cryptologic Research (IACR)" so we will attach our name to the award.

LaMacchia suggests that if we want to do this then we should be involved somehow. Yung explains that the awards committee can be extended. Abe states that we should have some sort of control over this award if we proceed. McCurley mentions that it might make sense if our test-of-time committee participates. Stebila mentions that he doesn't think it is necessary that the IACR has a direct vote for this award but we should have some observer from the IACR. This could either be someone from the test-of-time committee or someone from the Board (such as Yung).

Since there is insufficient time to discuss this further it is concluded that Yung will present a rewording of the proposal based on the current feedback and this will be concluded at the next Board meeting.

4. CLOSING MATTERS

Abdalla closes the meeting at 18h12 CEST.