MINUTES IACR BOARD MEETING *VIRTUAL-10 '21*

13 OCTOBER 2021

1. Opening Matters

1.1. **Welcome, roll of attendees, identification of proxies.** At 16h03 CEST 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 Rijmen holding proxy for Preneel and Stebila holding proxy for Schwabe. These minutes are reordered to the original agenda for consistency. LaMacchia requests to put an additional topic on the agenda related to the organizational structure.

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); Tancrède Lepoint (Director 2021-2023); Anna Lysyanskaya (Director 2019-2021); Francois-Xavier Standaert (Director 2020-2022, *CHES* Steering Committee).

Attendees (Appointed). Foteini Baldimtsi (Communications Secretary (2019-2022)); 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)); Vincent Rijmen (Journal of Cryptology Editor-in-Chief 2021–2023). 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). Bart Preneel (Director 2020-2022, *FSE* Steering Committee); Peter Schwabe (Director 2020-2022).

Absentees (Appointed). Lejla Batina (*Eurocrypt'20/'21* General Chair (2019-2021)).

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-9 '21.*

2. Votes

2.1. **Sponsorship of the RSA conference award.** The President recalls the proposal by Yung on behalf of Rivest and the *CT-RSA* Steering Committee. The proposal is for the IACR to become a co-sponsor for the "RSA Award for Excellence in Mathematics". Yung shared an updated version of the proposal by e-mail to the Board and asks for a vote of agreement such that we can move forward with this initiative. After a discussion it is clear that Abdalla, Yung and LaMacchia will work on a draft letter of agreement to set up a formal way of working for this award with the *CT-RSA* Steering committee.

Decision 2 (unanimous)**.** *The Board follows the proposal presented by Yung and agrees that the IACR becomes a sponsor for the "RSA Award for Excellence in Mathematics" handed out by the RSA Conference.*

2.2. **IACR new journal - next steps.** Bos provides an update from the New Journal committee: this includes a start of the cost and effort breakdown with different options for the New Journal. As communicated per e-mail Bos thinks it makes sense to vote if the Board in principle agrees to the creation of the New Journal. This allows us to present the intend of the Board at the Membership meeting at Eurocrypt and allows for a discussion.

Halevi asks if this vote includes decisions about the various technical details how the New Journal is implemented. Bos explains that all such decisions are not part of this vote and this is to be determined and decided later. Halevi remarks that he is not in favor of hosting the New Journal ourselves and that it would be wise to outsource this. Bos recalls that both options will be investigated and presented in an upcoming Board meeting.

Decision 3 (unanimous)**.** *The Board agrees in principle to the creation of the New Journal with as main goals*

- *Diamond or Gold Open Access publishing model*
- *Fast and consistent turnaround time (decision in 3 months for regular paper)*
- *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*
- *Not compete with but complement our successful flagship and area conferences (including the IACR transactions).*

3. Conferences

3.1. **Update on remaining 2021 conferences.** Picek provides an update on *Eurocrypt 2021*. There are already a large number of registrations for physical participation: 255. For the workshops around 150 people have registered. At the moment there is an increase in inquiries about what documents to bring for travel to Croatia. It is hard to give general advise since a lot of countries have their own (additional) rules. The President suggests to mail all registered participants a reminder of the Croatian rules. LaMacchia asks if the agenda is up-to-date since the Membership meeting seems to be missing. Picek clarifies that there has been time allocated for the Wednesday afternoon and that this has been flagged already and the website should be updated soon.

Halevi recalls that *TCC 2021* takes place in place in Raleigh, United States on November 8-11. This will be a hybrid event and organization is on-track. The program is up on the website.

Guo explains that the program for *Asiacrypt 2021* is being finalized. The President reminds him to not forget to schedule a time-slot for the Membership meeting.

LaMacchia gives an update on the status of *RWC 2022*. This will be a hybrid event in Amsterdam, the Netherlands. The reviews for the contributed talks are currently under discussion. They are looking at the *Eurocrypt* conference for the hybrid model and how many plan to attend physically.

4. Appointments, committees, and policies

4.1. **Election committee update.** Abe explains that the Election Committee finished setting up the election server. He thanks Lepoint and Stebila for their help. The website is also up and running thanks to Baldimtsi. There are six candidates for the three Director positions. The President thanks the Election Committee and all candidates for running.

5. 2023 Distinguished Lecture (to be delivered at *Crypto*)

The President recalls the Board needs to select a lecturer for the 2023 Distinguished Lecture at *Crypto* Several excellent candidates are nominated, and after discussion a candidate is selected.

Decision 4. *Hugo Krawczyk is appointed to give the Distinguished Lecture at Crypto 2023. [Krawczyk subsequently accepted.]*

6. Topics

6.1. **IACR Membership report.** Stebila presents the Membership report which has been shared with the Board before the Board Meeting. The IACR keeps growing and reached 3010 members in 2021. The registration system accommodates hybrid registration for conferences. For affiliated workshops this is not supported nor requested yet. The President thanks the Membership Secretary for all his work.

6.2. **Organizational Structure.** LaMacchia explains that he wishes to hire an attorney to see if the IACR can become a non-profit organization in another state. Currently the IACR is based in Nevada and this does not allow us to use various financial services for cheap money transfer and currency exchange. He will get a number of options and present this the Board. The Board has no objections to this plan.

7. Closing Matters

Abdalla closes the meeting at 17h31 CEST.