MINUTES IACR BOARD MEETING *VIRTUAL-6 '21*

16 JUNE 2021

1. Opening Matters

1.1. **Welcome, roll of attendees, identification of proxies.** At 16h02 CEST Abdalla opens the meeting and briefly goes around for an introductory round, confirming attendees and establishing who is holding proxies. There are 20 full time attendees with the following proxies: Stebila holds Bos's proxy; Rijmen holds Preneel's proxy until he arrives; Standaert holds Yung's proxy; Heninger holds Bishop's proxy; Lepoint holds Kolesnikov's proxy when he leaves; Schwabe holds Batina's proxy when she leaves.

1.1.1. *Roll of Attendees.*

Attendees (Elected). Michel Abdalla (President 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); 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)); Colin Boyd (*Eurocrypt'22* General Chair previously *Eurocrypt'21* General Chair (2020-2022)); 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));

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

Absentees (Elected). Joppe Bos (Secretary 2020-2022); Moti Yung (Director 2021-2023, *PKC* Steering Committee).

Absentees (Appointed). Allison Bishop (*Crypto'22* General Chair (2021-2022));

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. *The Board approves the Minutes of the IACR Board Meeting Virtual-5 '21 with one abstention (Lysyanskaya).*

1.3. **Review action items.** The following action items from past events remain open:

> Action Point **1: President** *(no time set)*:
> Create a concrete proposal for the Test-of-Time awards for the 1980s and 1990s papers. Preneel and Abe will join this Committee.

> Action Point **2: Yu** *(no time set)*:
> Look into the Bilibili video sharing platform and present a proposal if this fits the IACR's needs.

> Action Point **3: President** *(no time set)*:
> Contact the Dutch NWO to explain the current situation with respect to copyright at the IACR. Schwabe can assist if needed.

> Action Point **4: Lysyanskaya** *(no time set)*:
> Circulate proposed amendments from the Ethics Committee.

2. CONFERENCES

2.1. ***RWC* 2024 Proposal.** Stebila presents the *RWC'24* proposal for Toronto. Lysyanskaya asks about the motivation for presenting two bid options; LaMacchia notes that we have not yet had a chance to get eyes on the venues in person due to Covid restrictions. Abdalla asks if the price and attendee estimates are in line with previous RWCs; RWC 2019 (San Jose) had 642 attendees at USD$220, and RWC 2020 (New York) had 655 attendees at USD$230. Stebila leaves the call to allow the Board to discuss, then rejoins.

Decision 2. *The Board approves the proposal to host RWC 2024 in Toronto.*

2.2. **Update on 2021 conferences.** Kolesnikov provides an update for *Crypto*. Sponsorship is going fine. McCurley may have a conflict during the week of *Crypto* but Kay McKelly will be present to assist. Kolesnikov would like to know about the ability to use sponsorship money for affiliated events. LaMacchia notes that spending of sponsorship funds raised by the GC are at the discretion of the GC, subject to any agreements with the sponsor on how their contribution is to be spent, and to any other IACR policies.

Schwabe provides an update for *CHES*. The final batch of accepted papers received notifications today, and the program will be set later this week. McCurley is investigating whether online sponsor booths will be an option.

Batina provides an update for *Eurocrypt*. Batina expects that restrictions on hosting in-person events will be lifted in time for the Eurocrypt. Batina would like to update the conference website to begin listing visa and travel information. McCurley notes that the registration system may need some changes to handle the hybrid setting of both remote and local attendees; Stebila and McCurley to discuss. Standaert reports that the live talk format will be closer to the format used for online conferences, with a single track of shorter in-person talk with longer question/discussion sections, and full-length talk videos available online. If there are a large number of in-person registrations, a multi-track format may be considered. Schwabe has 3–4 in-person workshops confirmed and has several more under consideration; McCurley requests material on the affiliated events for the website.

Guo notes that no decision has been made for the format of *Asiacrypt*. The hope is to make it hybrid, but Singapore currently has many closures at the moment due to Covid. A decision is expected by end of July or early August.

RWC 2022 is currently proceeding as planned for an in-person event.

There are no updates for *TCC* or *FSE*.

3. APPOINTMENTS, COMMITTEES, AND POLICIES

3.1. **Asiacrypt 2023 program co-chair appointment.** The President recalls the Board needs to select the Program Co-Chair for *Asiacrypt 2023*. Several excellent candidates are nominated, and after discussion a candidate is selected.

Decision 3. *Ron Steinfeld is appointed Program Co-Chair for Asiacrypt 2023. [Steinfeld subsequently accepted.]*

The Board needs to select a member for the Test-of-Time Award Committee to replace Ueli Maurer who will be on the committee in 2022 and 2023, and chair the 2023 committee. Several excellent candidates are nominated, and after discussion a candidate is selected.

Decision 4. *Kazue Sako is appointed to the Test-of-Time Award Committee. [Sako subsequently accepted.]*

4. TOPICS

4.1. **Copyright discussion.** Rijmen reports on some issues with copyright regarding the Journal of Cryptology. Paterson noticed in 2019 that no one has been collecting copyright forms for papers in JoC, perhaps dating to early 2000s. We are now collecting copyright forms in which authors transfer copyright to the IACR. However, Rijmen notices that Springer seems to have a different view, with three types of copyright notices seen: 1) copyright to the IACR; 2) copyright to the authors; 3) copyright to the authors with exclusive license to the IACR. There is a subsequent copyright form that authors sign with Springer, which includes an author-paid open access fee, and which includes either a copyright transfer or a license-to-print. Lysyanskaya asks if prior to 2019 authors were signing Springer copyright forms; no answer is known. Rijmen says the core questions are (a) whether it is important for IACR to have the copyright or just a license to publish; and (b) whether Springer is collecting open access fees unnecessarily. Preneel notes that JoC is not open access, only that it is freely available to members.

> Action Point **5: President, Preneel, McCurley, Rijmen** *(no time set)*:
> Review the current agreement and identify next steps.

5. CLOSING MATTERS

Abdalla closes the meeting officially at 18h08 CEST. An informal discussion on software for the new journal follows among some members of the Board.