MINUTES IACR BOARD MEETING *VIRTUAL-8 '20*

14 OCTOBER 2020

1. Opening Matters

1.1. **Welcome, roll of attendees, identification of proxies.** At 23h00 CEST Abdalla 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 Abe holding proxy for Guo. When Lysyanskaya leaves (12h45) Reyzin has her proxy. Preneel joins at 23h25. These minutes are reordered to the original agenda for consistency.

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); Joppe Bos (Secretary 2020-2022); Masayuki Abe (Director 2018-2020); Nadia Heninger (Director 2019-2021); Tancrède Lepoint (Director 2018-2020). 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); Moti Yung (Director 2018-2020, *PKC* 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)); Vladimir Kolesnikov (*Crypto'21* General Chair (2020-2021)). Kenny Paterson (Journal of Cryptology Editor-in-Chief 2017–2020, *RWC* Steering Committee); Leo Reyzin (*Crypto'20* General Chair (2019-2020)); Douglas Stebila (Membership Secretary (2017-2020)).

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

Absentees (Elected). Marc Fischlin (Director 2020-2021);

Absentees (Appointed). Jian Guo (*Asiacrypt'21* General Chair (2020-2021)); Kwangjo Kim, (*Asiacrypt'20* General Chair (2019-2020));

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-7 '20.*

2. Appointments, committees, and policies

2.1. **IACR Election update.** The Chair of the Election Committee provides an update on the current status. All is going as planned and the website is up and running. The President suggests we should sent out a reminder to vote. Baldimtsi remarks that this is already planned for later this evening. The President asks how many members are eligible to vote. The Membership Secretary answers that 2490 can vote in this election. McCurley notes that our e-mail system might break when sending to so many people. He suggests to announce that each eligible member should have received credentials in an IACR news item. Baldimtsi confirms this is planned as well.

3. Status of conferences

3.1. **Update on forthcoming conferences (FSE / TCC / ASIACRYPT / RWC) GCs / SC liaisons.** The President recalls that all the upcoming conferences for this year are virtual. The reimbursements of the original registration fee of *FSE* earlier this year is almost complete. Additional information was needed for the reimbursement of a couple of payments and the Treasurer explains this will be taken care of soon. The virtual event of *FSE* will take place half a year later in November 2020: therefore it will include six issues of the Transactions.

Halevi recalls that *TCC* is virtually co-located with *FOCS*. Everything is on-track. More information is needed with respect to the affiliated workshops and this should be put on the webpage.

Kim is not present to provide an update on *Asiacrypt*. Abe also has no further information.

Paterson explains that the exact format of *RWC* is being discussed. The submitted talk proposals are underway. Paterson remarks that Usenix is running into financial issues due to the paid dedicated staff. We need to keep an eye on these developments and learn. The situation of the IACR is different since there is no paid staff and we were lucky with our venues where we could move events to the next year.

3.2. **Discussion about 2021 conferences.** The President states that we need to carefully consider how to proceed in 2021. The travel restrictions will be a reality for the upcoming future. We need to think about hybrid conferences.

Batina recalls that we don't have significant commitments for *Eurocrypt'21* except for a minor down-payment. The President wonders how realistic a physical event is in May 2021. Batina agrees this is hard to predict but we don't need to decide now.

For *PKC* we are considering a Plan B for moving to a virtual event. Once more information is known this will be aligned with the Board.

For *Crypto* there are no concerns at the moment: UCSB is flexible. Kolesnikov asks when to start discussing this with UCSB. Reyzin suggests that the December / January time-frame would be good.

It is unclear if the contract for *CHES* has been signed already and what the exact cancellation policy is. Standaert will ask the CHES Steering Committee for more information.

The President thinks that *Asiacrypt'21* is the most realistic event which can take place physically. It is remarked that we hope to hold *TCC'21* as a physical event as well. McCurley suggests we take into consideration the possibility that not all people will be able to get visas in a post-corona era due to travel restrictions.

Abe wonders what the technical difficulties are for a hybrid conference. McCurley answers that if we have sufficient internet connectivity and online support we can make it work.

4. Topics

4.1. **Communication issues.** Baldimtsi recalls that our policy for job postings is that only members of the IACR can post. However, for the announcement of events we have no such policy. This is inconsistent and we do not follow our own policy in practice. She proposes to change and unify this policy. There follows a discussion about ethics violations and if such members are allowed to post announcements. It is agreed that we change the policy such that everybody can post as well for the job postings as well as for the announcements of events.

Another topic relates to the IACR Twitter account. Currently, this also tweets all the new ePrint papers and important IACR news items get buried in all the tweets. Baldimtsi proposes to create a separate Twitter account for the announcement of new ePrint papers. There is broad support on the Board for this suggestion. Moreover, multiple conferences have separate Twitter accounts registered: some which are quite dormant. We need to better organize how we handle these accounts. LaMacchia remarks this is broader than just Twitter, the IACR also has a LinkedIn page for which he currently is the sole administrator. He proposed to add Baldimtsi as a second administrator. There follows a discussion if we should automate posting content to various social media platforms. In the end it is concluded that we focus on a couple main social media platforms and that we can handle this ourselves for now.

4.2. **New journal proposal update.** Bos explain that the New Journal Committee has been formed and that Christian Cachin agreed to join as co-chair. Nigel Smart and Elisabeth Smart joined as representatives of the authors of the proposal. An initial virtual meeting is planned for this week to discuss the goals and the motivation of this journal. The President thanks Bos for taking the lead and the initiative.

4.3. **HotCRP.** McCurley states that there is not much new to report. Each volume of both TCHES and FSE needs a new instance which needs to be setup. It is nearly impossible to add new features due to the undocumented and commented code-base. The President states that we need someone else to assist in adding features or help out with HotCRP. As a consequence the current policy is to reject any new feature request.

4.4. **Access to IACR videos from China.** McCurley and LaMacchia discuss the access to our videos in China. Although we want to reach as many people as possible we should not give control of our videos away. McCurley is happy to provide alternate means to share our videos if we keep control. Halevi suggests we ask Yu for his expertise.

> Action Point **1: President** *(no time set)*:
> Ask Yu about his recommendation on how to best share videos in Asia.

5. Closing Matters

Abdalla closes the meeting at 01h02 CEST.