

MINUTES IACR BOARD MEETING VIRTUAL-9 '20

12 NOVEMBER 2020

1. OPENING MATTERS

1.1. Welcome, roll of attendees, identification of proxies. At 22h11 CEST Abdalla opens the meeting and briefly goes around for an introductory round, confirming attendees and establishing who is holding proxies. There are 21 full time attendees with LaMacchia holding proxy for Heninger, Halevi for Lepoint and Abe for Guo. When Baldimtsi has to step out Lysyanskaya holds her proxy and vice-versa. 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); Marc Fischlin (Director 2020-2021); 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); 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)); Kwangjo Kim, (*Asiacrypt'20* General Chair (2019-2020)); Vladimir Kolesnikov (*Crypto'21* General Chair (2020-2021)). 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). Nadia Heninger (Director 2019-2021); Tancredè Lepoint (Director 2018-2020).

Absentees (Appointed). Jian Guo (*Asiacrypt'21* General Chair (2020-2021)); Kenny Paterson (Journal of Cryptology Editor-in-Chief 2017–2020, *RWC* Steering Committee);

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-8 '20.*

2. CONFERENCES

2.1. Renewal of insurance policies. LaMacchia recalls that we have a general liability insurance as well as a dedicated director and officer liability insurance. These are about to expire and he has asked for new quotes including the increased assets. The Treasurer is preparing the annual non-profit tax return, as soon as it is ready it will be shared with the Board for review. The President asks to share the new quotes with the Board over e-mail.

2.2. CHES 2021 & 2022 new dates approval. The *CHES* Steering Committee is recommending to shift their program by one year. This means

- *CHES 2021* will take place in Beijing, China with General Chairs Liji Wu, Zhe Liu, Guoqiang Bai, and Junfeng Fan (which was confirmed for *CHES 2020*)
- *CHES 2022* will take place in Prague, Czech Republic with General Chairs Hana Kubátová and Martin Novotný (which was confirmed for *CHES 2021*)

There is a brief discussion about the problems with transferring money to China. The Treasurer explain that this is expected to be easier now since this goes through the university. We are waiting for the contract to be reviewed for the 2022 venue. It is agreed that the *CHES* Steering Committee should share this with the Treasurer.

Action Point 1: **Standaert** (*no time set*):

Check the status of the venue contract of *CHES 2022* and share this with the Treasurer.

Decision 2 (unanimous). *The Board approves the recommendation of the CHES Steering Committee to move the schedule of CHES 2020 and CHES 2021 one year forward.*

2.3. **Update on forthcoming conferences (FSE / TCC / ASIACRYPT / RWC).** *FSE* is taking place this week. McCurley recalls that the time-zone is good for Asia and Europe but not really for the USA. The sessions go really well.

The next conference is *TCC*. The preparations for the training sessions are underway. After this *Asiacrypt* is up, everything is going as expected. Kim mentions that the program for *Asiacrypt* is almost finished. They are currently discussing an idea to have dedicated Asian language rooms.

There seems to be a delay with the DOI provided by Springer. This happened earlier this year for *PKC* as well. The fallback option is to refer to the ePrint papers. The automatic upload feature to upload to ePrint in websubrev is broken. Halevi will have a look at this. The authors have been told to upload to ePrint and Bos will assist to get them online as soon as possible.

LaMacchia mentions that the draft program for *RWC* is ready.

3. APPOINTMENTS, COMMITTEES, AND POLICIES

3.1. **Election committee update.** Lysyanskaya provides an update on behalf of the Election Committee. Except for a typo in one of the names everything went smoothly. Fischlin suggests to send out a reminder to vote tomorrow morning.

3.2. **2021 Fellows committee update.** The Fellows Committee recalls that the term of Chris Peikert has ended and that Daniele Micciancio joined the Committee. The nominations for the Fellows has not been advertised too much yet. The deadline has been extended until December 1st. Baldimtsi will send out a reminder after the election.

3.3. **Distinguished Lecture to be held at Eurocrypt 2022.** The distinguished lecture is held annually, on invitation by the Board. Its location cycles between the three IACR general conferences. Several excellent candidates are nominated, and after discussion a candidate is selected.

Decision 3 (unanimous). *Ingrid Verbauwhede is invited to deliver the Distinguished Lecture at Eurocrypt'22. [Verbauwhede subsequently accepted.]*

4. TOPICS

4.1. **Test-of-Time awards for older papers.** Yung received the IEEE S&P 2020 Test of Time award where multiple papers are selected from past decades. Other venues hand out such awards in ten year increments for older papers. The President asks the Board about their opinion about this approach. There follows a discussion; this is a hard job for the Committee and what time periods do we want to consider? The Board thinks this is worth pursuing and the President will investigate the best way forward.

Action Point 2: **President** (*no time set*):

Propose the way forward for the Test-of-Time Award for older papers.

4.2. **New journal proposal update.** Bos updates the Board about the recent progress. The New Journal subcommittee has had one virtual meeting. The main goal, impact on other venues, reviewing process and hosting possibilities have been discussed. The next meetings are already planned. McCurley is currently experimenting with the Open Journal System. The President thanks Bos for taking the lead here.

5. CLOSING MATTERS

Abdalla closes the meeting at 10h49 CEST.