

MINUTES IACR BOARD MEETING VIRTUAL-4 '20

3 JUNE 2020

1. OPENING MATTERS

1.1. Welcome, roll of attendees, identification of proxies. At 16h05 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. Preneel joins the meeting at 16h34 CEST. Reyzin leaves the meeting at 17h23 CEST and Lysyanskaya has his proxy.

1.2. Review and approval of agenda. The agenda is approved, with the understanding that the meeting will be held in an order slightly deviating from the agenda (as certain items have scheduling constraints). These minutes are reordered to the original agenda for consistency.

1.2.1. 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); Marc Fischlin (Director 2020-2021); 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* General Chair (2019-2020)); Colin Boyd (*Eurocrypt'21* General Chair (2020-2021)); Jian Guo (*Asiacrypt'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)); Vladimir Kolesnikov (*Crypto'21* General Chair (2020-2021)).

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

Absentees (Elected). Masayuki Abe (Director 2018-2020);

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

Absentees (Representatives and Others). Hilarie Orman (Archivist); Tal Rabin (Code-of-conduct Liaison);

1.3. Approve minutes from last BoD virtual meeting. The President thanks the Secretary for the completion of the minutes which have been shared before the 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-3 '20.*

2. APPOINTMENTS, COMMITTEES, AND POLICIES

2.1. CHES 2020 General Chairs approval. The President recalls that the Board needs to vote on the suggested two General Chairs for *CHES 2020* by the *CHES* Steering Committee since this event will be run virtually. There is a short discussion about the two candidates.

Decision 2 (unanimous). *The Board follows the recommendation from the CHES Steering Committee and appoints Chuengsatiansup and Yarom as General Chairs for CHES 2020.*

2.2. Program Chair list maintenance. The President explains his initiative for a new way of voting for the Program Co-Chairs which was shared before the Board Meeting per e-mail. The goal is to make the process more robust: in the elimination phase (when the number of candidates is more than three) each elected Board Member gets to vote on two different candidates instead of one.

2.3. EUROCRYPT program co-chair appointment. The President recalls the Board needs to select a second Program Co-Chair for *Eurocrypt 2022* which will serve with Orr Dunkelman. Several excellent candidates are nominated, and after discussion a candidate is selected.

Decision 3. *Stefan Dziembowski is appointed Program Co-Chair for Eurocrypt'22. [Dziembowski subsequently accepted.]*

2.4. Crypto program co-chair appointment. The President recalls the Board needs to select the first Program Co-Chair for *Crypto 2022*. Several excellent candidates are nominated, and after discussion a candidate is selected.

Decision 4. *Thomas Shrimpton is appointed Program Co-Chair for Crypto'22. [Shrimpton subsequently accepted.]*

2.5. Test-of-Time Award Committee. The Test-of-Time Award Committee in any year includes two members appointed by the IACR Board of Directors, and three program chairs of the current year's IACR general conferences as ex-officio members. An award will be given at a conference for a paper which has had a lasting impact on the field and was published 15 years prior.

The President explains that we are looking for a replacement of Tatsuaki Okamoto; the new Chair of the Test-of-Time Award Committee will be Ueli Maurer. Several excellent candidates are nominated, and after discussion a candidate is selected.

Decision 5. *Nigel Smart is appointed to be part of the Test-of-Time Award Selection Committee. [Smart subsequently accepted.]*

2.6. JoC Editor-In-Chief update. The Committee consisting of Paterson, Abe, Standaert, and Abdalla responsible for finding a replacement of the current JoC Editor-In-Chief present their finding and recommendations. After careful considerations a short list is presented to the Board. There follows a discussion about the recommendations and the candidates.

Decision 6. *Vincent Rijmen is appointed the new JoC Editor-In-Chief for a three year term. [Rijmen subsequently accepted.]*

2.7. Status of conferences. McCurley present the slides made McKelly and himself providing an update on virtual conferences. The presentations went over the things we learned from *Eurocrypt* and how to apply this to the upcoming virtual events.

There is a discussion related to the cost recovery. The Treasurer explains that the direct costs of a virtual conference are low and we could likely cover those costs with a small per-event registration fee (on top of the IACR Membership fee). The Treasurer estimates that a registration fee in the range of USD 10-20 would likely be sufficient to cover the cost of organizing an event virtually. The Treasurer further suggests that, if a non-zero registration fee is imposed, then it should only apply to Regular registrations and that the IACR should continue to make Student registrations for virtual events free (beyond the IACR Student Membership fee).

The President wants that *FSE* and *TCC* look into options which allow remote participation. Such hybrid conferences would be very welcome. Preneel points out that this is not always possible: not all venues / hotels have good enough internet.

McCurley presents the ongoing work related to HotCRP versus websubrev. The President wants to make a good and fair comparison before we invest too much time into this. Halevi points out that they have distributed a survey and hope to get sufficient information to make an informed decision. This discussion related to HotCRP versus websubrev is to be continued. The President calls for feedback and input.

3. CLOSING MATTERS

Abdalla closes the meeting at 18h03 CEST.