

MINUTES IACR BOARD MEETING *VIRTUAL-2 '20*

1 APRIL 2020

1. OPENING MATTERS

1.1. **Welcome, roll of attendees, identification of proxies.** At 16h04 CET Abdalla opens the meeting and briefly goes around for an introductory round, confirming attendees and establishing who is holding proxies. There are 22 full time attendees with no one holding proxies.

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); Masayuki Abe (Director 2018-2020); Marc Fischlin (Director 2020-2021); Nadia Heninger (Director 2019-2021); Tancrede 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)); Kwangjo Kim, (*Asiacrypt'20* General Chair (2019-2020)); 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 (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);

1.3. **Approve minutes from last BoD virtual meeting.** The President thanks the Secretary for completing the minutes in a timely manner and sharing this with the Board.

Decision 1 (unanimous). *The Board approves the minutes of the Virtual-1 2020 Board meeting.*

2. APPOINTMENTS, COMMITTEES, AND POLICIES

2.1. **Election committee update.** The President recalls he has an action point to form the Election Committee. In the last virtual Board meeting Lysyanskaya and Preneel volunteered but a third person is needed.

2.2. **JoC Editor-in-Chief update.** The President recalls that the Board needs to look for a replacement of Kenny Paterson. Paterson was supposed to step down last year but agreed to a one year extension. Abdalla informs the Board that the committee to look for a JoC EiC replacement currently consists of Abdalla, Paterson, Abe, and Standaert. More volunteers are welcome to join this committee and the President asks to contact him if there is an interest.

3. STATUS OF CONFERENCES

The status of the upcoming conferences have been separated in three categories.

3.1. Postponed conferences: EUROCRYPT, FSE, PKC. *Eurocrypt 2020* will be IACR's first all-digital event. The plan is to move the schedule by one year: hosting *Eurocrypt 2021* in Croatia and *Eurocrypt 2022* in Norway. Colin informs the Board they are looking into two possible dates for *Eurocrypt 2022*. He prefers to shift the conference to late May. Yung agrees that later is better to avoid a potential second wave of the coronavirus. LaMacchia recalls that May 30 is memorial day in the USA and Preneel asks whether Easter coincides with the proposed dates. Colin explain that these dates have been checked and do not overlap with Easter. The President asks the General Chair of *Eurocrypt 2021* if he has a strong preference: this is not the case. The President wants to move this discussion offline. Halevi recalls that typically the GC proposes a date and the Board approves / disapproves. Abdalla agrees and asks Colin to propose a date such that the Board can make a decision.

For *FSE 2020* there is no update to report. The conference is postponed to November since everything was paid already.

The Steering Committee and the General Chair of *PKC 2020* are considering to switch to an all-digital event and use the same venue next year or, alternatively, host *PKC 2020* in the fall.

3.2. Conferences likely to be canceled: CHES, CRYPTO. Reyzin explains that we can switch to a all-digital *CRYPTO 2020* conference without significant impact. He suggests to make a final decision by the end of May. McCurley suggests a hybrid solution where members can join in-person and digitally. Reyzin agrees and this option is under investigation. Currently the *CRYPTO 2020* webpage has an advise against making any non-refundable expenditures. There follows a discussion about how and when to update the webpage. Reyzin suggests to post the decision after the self-imposed deadline in May. Reyzin points out that the hybrid solution for the conference is by far the most expensive solution. The Treasurer agrees but wants to discuss this at a later point. The President wants to have a decision by the end of May at the latest since our members should know what to expect in case they want to make travel arrangements.

The Presidents summarizes the ongoing discussion with the CHES Steering Committee. The preference seems to be to postpone the conference: either a full year or to March next year. The problem with a CHES conference twice next year is that it is expected that not many people from industry will attend both events. If the decision is to postpone then it is likely this will be by one year. One idea is to allow authors to present at next year CHES if they want. Batina informs if this is allowed or policy since this might have implications for Eurocrypt as well. The Presidents believes such large conferences with three or four tracks do not seem realistic. Yung stresses that the virtual events should be complete no matter what.

3.3. Other conferences: TCC, ASIACRYPT, RWC. Halevi explains that there are ongoing discussions with the TCC venue to allow for cancellation options by August. *TCC 2020* is co-located with FOCS which seems to take place. Reyzin asks how the organizers of FOCS handle the current situation. It seems that IEEE negotiated the option to cancel the events without a financial impact.

For *Asiacrypt 2020*, Kim explains that no decisions have been made. Moreover, no financial commitments have been made since the contract has not been signed. They prefer to watch and see what *Crypto 2020* will decide. The hybrid solution is definitely an option.

For *RWC 2021* the contract has already been signed with the venue. Schwabe explains that they are looking for possible alternative dates in 2021. LaMacchia thinks it is too soon to already consider possible alternatives for RWC.

4. TOPICS

4.1. Handling of canceled events. LaMacchia would like to thank Stebila for implementing an uniform way to handle our refund policy. Stebila created a script which can process bulk refunds. The impact for the members is that for non-US currencies there can be a currency fluctuation and credit card companies might charge conversion fees. LaMacchia will perform a test-trial for *PKC*. LaMacchia suggests to roll-over the sponsorship received to the next edition.

Decision 2 (unanimous). *LaMacchia and Stebila are responsible and allowed to process the bulk refunds.*

There follows a discussion how to ensure to keep our current members if we do virtual conferences. We should have the option to allow for a digital payment of the membership fee when participating.

4.2. Start time for next virtual board meeting.

Action Point 1: Abdalla (no time set):
Create a Doodle for the next virtual meeting(s) + exact time.

4.3. **Move to virtual conferences.** McCurley and McKelly present slides regarding different aspects when moving from physical to virtual conferences. Different requirements are presented and discussed. Both McCurley and McKelly will meet with Program Chairs and General Chairs to coordinate activities and review plans. Reyzin raises the idea of watch parties so members can watch presentations together and discuss them. McKelly explains this was not considered and likes the idea.

The President thanks McCurley and McKelly for all their preparation work and starting this discussion. This topic will stay on the agenda for the next Virtual Meeting.

5. CLOSING MATTERS

Abdalla closes the meeting at 18h18 CET.