MINUTES IACR BOARD MEETING *VIRTUAL-2 '21*

10 FEBRUARY 2021

1. OPENING MATTERS

1.1. **Welcome, roll of attendees, identification of proxies.** At 16h00 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 no-one holding proxies. 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 2021-2023); Marc Fischlin (Director 2020-2021); Nadia Heninger (Director 2019-2021). 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 2021-2023, *PKC* Steering Committee).

Attendees (Appointed). Foteini Baldimtsi (Communications Secretary (2019-2022)); Lejla Batina (*Eurocrypt'20/'21* General Chair (2019-2021)); Allison Bishop (*Crypto'22* General Chair (2021-2022)) 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). Tancrède Lepoint (Director 2021-2023);

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-1 '21.*

2. CONFERENCES

The President recalls that *PKC'21* has requested to go virtual. Yung explains that the organizers of this year's *PKC'21* has carefully examined options for the conference, and would like to proceed to host the conference virtually on the planned dates of May 10-13, 2021.

Decision 2 (unanimous)**.** *The Board approves the proposal by the PKC organization committee to host the conference virtually on May 10-13, 2021.*

2.1. **Discussion about other 2021 conferences.** Kolesnikov provides an update regarding *Crypto'21*. He has contacted UCSB for an update. The university seems not very comfortable with external programs coming to campus this summer. Halevi believes their mood might change before the summer. The President states that we can proceed as planned for the moment: there is no need to make a decision about this yet.

Kolesnikov asks what kind of support for the workshops / affiliated events we want to offer. For example, do we allow them to use our virtual platform? The President recalls we used the virtual platform also for the affiliated events last year. McCurley suggests that the sponsorship income can cover for these additional expenses. The Treasurer believes that the cost for the licenses of the software is minimal compared to the time and effort spent by an IACR contractor. He asks how many affiliated events are foreseen. It seems there is a preference for two affiliated events per day and then we can budget for this accordingly.

Schwabe explain that the affiliated event situation for *Eurocrypt* is more complicated. It is foreseen that 10 workshops will be moved to this year from last year. Some already indicated that they want to run hybrid. The President believes running hybrid affiliated workshops will be too high a risk for the IACR. Batina stresses that many of the affiliated events are only interested if the workshop takes place physically. Schwabe suggests to create a plan how to inform the workshop organizers. There follows a discussion how to approach this best and what to put in the call for proposals. It is concluded that the affiliated events are a valuable addition to the main event. The call for proposals remains as-is and the costs for these events will be recovered through sponsorship or a registration fee. We will not commit yet to the organization of hybrid affiliated events in the call for proposals. The potential issues for *Eurocrypt* will be discussed later.

Standaert updated the Board on the status of *CHES*. He has asked the organizers about a status update. He is waiting for the Steering Committee meeting which will provide an update.

3. Appointments, committees, and policies

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

Decision 3. *Carmit Hazay is appointed Program Co-Chair for Eurocrypt 2023. [Hazay subsequently accepted.]*

4. Topics

4.1. **IT Asset report.** McCurley shares a presentation of the IT status. The main message is that we need to migrate away from our old server and use the opportunity to separate services on different machines. Halevi suggests we set a deadline otherwise this will not happen. It is agreed to find new people who want to join the IT Committee. The IT Committee will make a plan to migrate the server and in parallel the Board searches for new peopel interested in joining this Committee.

4.2. **IACR Copyright.** Schwabe explains that many European funding bodies have started “Plan S”, an initiative to further promote open-access publishing. Researchers with grants from these funding bodies are required to publish their work with open-access plans, otherwise parts of their funding will be cut. While the goals of Plan S are very much in line with the mission of the IACR, the implementation of Plan S in some countries (e.g., the Netherlands) is probably incompatible with the copyright form that we ask authors to sign for IACR venues. Specifically, NWO, the Dutch research funding organization, interprets Plan S as “copyright must remain with the authors”.

There follows a discussion about the current IACR copyright situation. It is clear this is not a problem for the IACR Transactions but for our other venues. It is recalled that the IACR currently does take copyright for a reason: when someone working at industry writes a paper the company automatically get the copyright of the author and if this author leaves the company then various problems arise. It is suggested that the IACR should be flexible and allow for multiple copyright options. For the IACR it is most important that all our papers appear free for the public on the ePrint Archive. It is suggested to ask the Dutch NWO why they demand the copyright to remain with the authors. The best time to renegotiate this with Springer would be when we renew our contract. If we plan to do this we need a solid plan and strategy.

Action Point **1: President** *(no time set)*:
Contact the Dutch NWO to explain the current situation with respect to copyright at the IACR.

4.3. **EUROCRYPT 2023 search.** The President suggests to use our network to look around for proposals for *Eurocrypt 2023* after we have *Eurocrypt 2021* in Croatia and *Eurocrypt 2022* in Norway.

5. Closing Matters

Abdalla closes the meeting at 17h59 CEST.