MINUTES IACR BOARD MEETING *VIRTUAL-1 ’22*

27 JANUARY 2022

1. Opening Matters

1.1. **Welcome, roll of attendees, identification of proxies.** At 21h07 CET Abdalla opens the meeting and briefly goes around for an introductory round, confirming attendees and establishing who is holding proxies. There are 18 full time attendees with Yang holding proxy for Guo, LaMacchia for Stebila when absent and Preneel for Rijmen. Yung joins the meeting at 21h22 and Preneel joins the meeting at 22h00. These minutes are reordered to the original agenda for consistency.

1.1.1. *Roll of Attendees.*

Attendees (Elected). Michel Abdalla (President 2020-2022); Joppe Bos (Secretary 2020-2022); Shai Halevi (Vice President 2020-2022, *TCC* Steering Committee); Brian LaMacchia (Treasurer 2020-2022); Masayuki Abe (Director 2021-2023); Bart Preneel (Director 2020-2022, *FSE* Steering Committee); Tancrède Lepoint (Director 2021-2023); Anna Lysyanskaya (Director 2022-2024); Peter Schwabe (Director 2020-2022); Francois-Xavier Standaert (Director 2020-2022, *CHES* Steering Committee); Bo-Yin Yang (Director 2022-2024, *Asiacrypt’22* General Chair (2021-2022)); Moti Yung (Director 2021-2023, *PKC* Steering Committee).

Attendees (Appointed). Allison Bishop (*Crypto’22* General Chair (2021-2022)); Colin Boyd (*Eurocrypt’22* General Chair); Foteini Baldimtsi (Communications Secretary (2019-2022)); Britta Hale (*Crypto’23* General Chair (2022-2023)); Douglas Stebila (Membership Secretary (2017-2022)); Fangguo Zhang (*Asiacrypt’23* General Chair (2022-2023))

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

Absentees (Elected). Jian Guo (Director 2022-2024),

Absentees (Appointed). Vincent Rijmen (Journal of Cryptology Editor-in-Chief 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-12 ’21.*

2. Conferences

2.1. **Eurocrypt 2022.** Boyd provides an update on the organization of *Eurocrypt’22*. The contract of the conference hotel states that we are soon liable for 50 percent of the cost. His assessment is that the perceived risk is low and there is no need to cancel the contract. The President agrees with this assessment. The Treasurer highlights that we are very well aware of the financial risks but advises to be conservative with the number of physical attendees we promise to the venue. We can use *RWC* and *FSE* as examples. Boyd shows an outline of the foreseen high-level overview of the program. The most notable change is that the conference is shifted by one day compared to previous years: starting at Tuesday.

McCurley asks about the audio/video requirements for the conference given that we expect a large audience online. This will be discussed offline. Stebila request a separate meeting to discuss how VAT will affect the registration.

2.2. **Update on other upcoming conferences.** The plan for *FSE* is still to host this as a hybrid conference. Yung recalls that since the Japanese government decided to halt new entries from abroad, *PKC* is held virtually in March. Schwabe recalls that the registration for *RWC* has just re-opened and is planned as a hybrid conference with live streams. Bishop explains that *Crypto* will be a hybrid event. The plans for the social events have started. She is aligning with UCSB for the exact requirements on the vaccination status imposed by the university. The call for workshop proposals will be sent out later this week. Schwabe is interested in the vaccination discussion also for

RWC. There follows a discussion how to handle checking this vaccination status in a privacy sensitive way and comply with the requirements with UCSB.

Standaert announces that the CHES Steering Committee recommends to move *CHES* 2022 from Beijing, China to Leuven, Belgium. The President agrees that this makes sense and when more information is avaiable the Board will vote on this. Yang explains that we will have more clarity for *Asiacrypt* by midyear since there are still quarantine requirements in Taipei, Taiwan. The sponsorship is underway and going well. Also for *Asiacrypt* the plan is to shift the program by one day just as for *Eurocrypt*. Yang asks if it is desirable to co-locate with a large hacker event. The President asks if this would bring in more a more diverse group of participants. Yang assesses that this is the case assuming the event takes place in-person. This has not been done before and will be investigated in more detail.

2.3. **Eurocrypt 2023 Search.** The President summarizes the ongoing search for the *Eurocrypt* 2023 venue. One of the options was Leuven, Belgium but since CHES moved here this is no longer an option. The President asks the Board to use their network to ask for volunteers for both 2023 and 2024. Various options are discussed and the people involved will be contacted.

The President mentions that the Board received an e-mail from the Academy of Cryptography of the Russian Federation to hold *Eurocrypt* 2024 in Russia. This option is discussed and the Board concluded that 2024 would not be a good time to attempt to hold Eurocrypt in Russia, given the current environment and the fact that the IACR is legally registered in the US. Currently, there is a significant risk of structural impediments that would make it impossible to organize an event in Russia under the auspices of a US-based non-profit organization like the IACR. The President will communicate this message.

3. Topics

3.1. **Committee updates.** The Ethics Committee reports that Bishop and Lepoint joined. It is observed that the Schools Committee webpage needs to be updated.

3.2. **Subsidiary.** The Treasurer report back on the work related to the creation of the IACR subsidiary as discussed at the previous Board meeting with as main goal to make use of discounted currency conversion. This "IACR Services, LLC" has been successfully registered in the state of Washington.

The Treasurer asks for guidance with respect to timing risk for our investment policy. There follows a discussion and Bishop will discuss this with Treasurer in more details offline.

3.3. **Update on the new journal proposal.** Bos summarizes the work performed by the New Journal Committee. This included the foreseen split in three steps: (1) Submission & review, (2) Editing and (3) Hosting. As requested by the Board an updated cost proposal is presented which we received from Cambridge for step (3). There follows a discussion about the pros and cons of outsourcing this a third party versus doing everything ourselves. On the one hand there is a risk that we do not have sufficient volunteers to run this New Journal while on the other hand this would be an opportunity to re-use the ongoing rewrite of the Cryptology ePrint Archive by McCurley and create a common IACR platform. The discussion is concluded without any concrete decisions and Bos will take this up with the New Journal Committee and come back with a concrete proposal for the next steps.

4. Closing Matters

Abdalla closes the meeting at 23h05 CET.