

# MINUTES IACR BOARD MEETING VIRTUAL-4 '22

6 APRIL 2022

## 1. OPENING MATTERS

**1.1. Welcome, roll of attendees, identification of proxies.** At 17h02 CEST the President opens the meeting and briefly goes around for an introductory round, confirming attendees and establishing who is holding proxies. There are 19 full time attendees with Halevi holding proxy for Bishop (until she arrives) and for Lepoint (when he leaves). Malkin joins at 17h13 CEST. 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); Brian LaMacchia (Treasurer 2020-2022); Masayuki Abe (Director 2021-2023); Jian Guo (Director 2022-2024); Bart Preneel (Director 2020-2022, *FSE* Steering Committee); Tancrede 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). Colin Boyd (*Eurocrypt*'22 General Chair); Britta Hale (*Crypto*'23 General Chair (2022-2023)); Vincent Rijmen (Journal of Cryptology Editor-in-Chief 2021–2023). Douglas Stebila (Membership Secretary (2017-2022)); Fangguo Zhang (*Asiacrypt*'23 General Chair (2022-2023)).

*Attendees* (Representatives and Others). Tal Malkin (*TCC* Steering Committee); Kevin S. McCurley (Database Administrator).

*Absentees* (Appointed). Foteini Baldimtsi (Communications Secretary (2019-2022)); Allison Bishop (*Crypto*'22 General Chair (2021-2022));

*Absentees* (Representatives and Others). Mitsuru Matsui (*Asiacrypt* Steering Committee); Hilarie Orman (Archivist); Kenny Paterson (*RWC* Steering Committee); 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. Michel calls for a vote to approve the minutes.

**Decision 1** (unanimous). *The Board approves the Minutes of the IACR Board Meeting Virtual-3 '22.*

## 2. CONFERENCES

**2.1. Update on upcoming conferences.** Schwabe reports that they are ready for *RWC*, they aim for 500 to 550 physical attendees. Preneel reports no new for *FSE*. The registration for *Eurocrypt* has opened. Boyd announces that the registration fee is higher than expected due to VAT. They plan for two parallel sessions. There is a question if we plan for a physical Board Meeting. The President says this is currently planned for the Monday. Halevi urges to put the program online soon. No update on *Crypto* since Bishop is absent. No update for *CHES* from Standaert. No update for *TCC* from Malkin. She reports that there is a potential problem with the venue since they haven't heard back from them. This will be sorted out offline. Yang report that they almost settled on the venue for *Asiacrypt*, they are investigating a good cancellation policy.

## 3. TOPICS

**3.1. IACR School Proposal.** Lepoint presents the school proposal they received outside the regular cycle and was shared with the Board before the Meeting. Even if the school proposal was submitted outside of the normal deadline, the school committee considers that such efforts to organize an event in the middle of the pandemic after a break of two years should be encouraged to the maximum extend. The funding requested is USD 3000 and dedicated to help local out-of-town students to attend the school. The organizers have the experience from the previous two editions. The school committee makes the recommendation of funding the school up to the amount being requested.

The President asks about any COVID restrictions. Yang reports that quarantine restrictions are very likely and therefore foreign attendees seem not likely. Preneel supports this proposal and asks if virtual attendance will be possible. Yang reports this is indeed the case.

**Decision 2** (unanimous). *The Board follows the recommendation by the Schools Committee and decides to fund the Post-Quantum Cryptography Mini-School to be held in Taipei, Taiwan for 3000 USD.*

**3.2. Revised conflict of interest policy.** Stebila recalls the discussion and action from the previous Board meeting to clarify our CoI. Stebila shows the suggested changes which have been shared with the Board before the meeting. There follows a discussion to include an undergraduate thesis in the scope of the CoI. There follows a vote to consider the Bachelor thesis as an automatic conflict which does not pass.

**3.3. Statement Ukraine.** Halevi present the draft statement condemning the Russian war in Ukraine, this was inspired by the text from the Institute of Mathematical Statistics. Guo asks if we should punish the research community in Russia by not affiliating with Russian conferences. He reasons that if we do it now we should do it consistently for other wars as well. There follows a discussion how to deal with future statements.

**Decision 3.** *The Board agrees to publish the following statement on the IACR website:*

*The IACR strongly condemns the unprovoked and unjust war that Russia is waging in Ukraine. We are outraged by the suffering and loss of life that this brutal aggression is inflicting on the Ukrainian People.*

*While this war continues, the IACR will not hold or plan to hold any conference in Russia, nor will it be affiliated with conferences in Russia.*

*The IACR fully endorses the following joint statement by the National Academies of G7 States which was published on 2 March 2022: "The unprovoked attack against Ukraine, a democratic and independent country, is a blatant violation of international law and of core values of humanity. The Russian invasion is an assault on the fundamental principles of freedom, democracy and self-determination, which provide the basis for academic freedom and opportunities for scientific exchange and cooperation.*

*In this dark hour, our thoughts and deepest sympathy are with the people of Ukraine. We are determined to support the National Academy of Sciences of Ukraine. We stand in solidarity with the scientific community and the scientists in Ukraine.*

*We acknowledge the Russian scientists and citizens who are ashamed of this attack and speak out against the war.*

*We call on the Russian leadership to immediately cease all military action against Ukraine and put an end to this war."*

**3.4. Eurocrypt 2024 program co-chair appointment (one name).** The President recalls that we need to appoint a Program Co-Chair for *Eurocrypt 2024*. Before the Board meeting several excellent candidates have been nominated, and after discussion a candidate is selected.

**Decision 4.** *Marc Joye is appointed Program Co-Chair for Eurocrypt 2024. [Joye subsequently accepted.]*

**3.5. New journal proposal Editor-in-Chief Role Discussion.** Bos updates the Board on an initial alignment call with Privacy Enhancing Technologies Symposium (PETS) since they also look into creating a new open access journal. The discussion on the role for the Editor-in-Chief is postponed due to a lack of time.

#### 4. CLOSING MATTERS

The President closes the meeting at 19h06 CEST.