MINUTES IACR BOARD MEETING *VIRTUAL-3 '22*

23 MARCH 2022

1. Opening Matters

1.1. **Welcome, roll of attendees, identification of proxies.** At 22h04 CET 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 Preneel holding proxy for Rijmen, Yang for Guo, Yung for Lysyanskaya, Stebila for LaMacchia (when not present), and Hale for Bishop (when not present). McCurley joins at 22h12 CET, LaMacchia at 22h57 CET and Bishop leaves at 23h08. 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); Bart Preneel (Director 2020-2022, *FSE* Steering Committee); Tancrède Lepoint (Director 2021-2023); 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). Foteini Baldimtsi (Communications Secretary (2019-2022)); Allison Bishop (*Crypto'22* General Chair (2021-2022)); Colin Boyd (*Eurocrypt'22* General Chair); 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). Tal Malkin (*TCC* Steering Committee); Kevin S. McCurley (Database Administrator).

Absentees (Elected). Jian Guo (Director 2022-2024); Anna Lysyanskaya (Director 2022-2024).

Absentees (Appointed). Mitsuru Matsui (*Asiacrypt* Steering Committee); Kenny Paterson (*RWC* Steering Committee); 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. Michel calls for a vote to approve the minutes.

Decision 1 (unanimous)**.** *The Board approves the Minutes of the IACR Board Meeting Virtual-2 '22.*

2. Conferences

2.1. **Update on upcoming conferences.** Preneel explains that *FSE* is currently running as a hybrid event. Everything goes smoothly thanks to the help of McCurley. Next year, the plan is to hold *FSE '23* from March 20-24, 2023 in Beijing, China. The FSE Steering Committee asks for a fallback plan and the location will be really confirmed 6 months in advance of the conference.

Schwabe mentions that there are already over 400 physical registrations for *RWC*. The Dutch government lifted all COVID restrictions. There follows a discussion if the IACR should encourage or mandate wearing masks at the conference. It is decided we will strongly encourage everybody who plans to attend *RWC* in person to have completed their vaccinations but not enforce any strict COVID measures.

Boyd also mentions that there are currently no COVID restrictions in Norway. The organization for *Eurocrypt* goes as planned. They are working to get the registration up before the end of the month. It is foreseen to hold a hybrid Board meeting on Monday. Boyd received a question from the PC chairs about a possible IACR statement around the war in Ukraine. Yung explains that we would need a concrete proposal to discuss if we want to move this forward in the Board. The current initiatives from other organizations seem to be meaningful. We will investigate and write a draft statement to be presented at the next Board meeting.

Action Point **1: Shai** *(no time set)*:
Create a draft IACR statement with respect to the war in Ukraine.

Bishop provides an update for *Crypto*. She found a replacement vendor for the Crypto Cafe. UCSB has relaxed the rules around proof of vaccination. This will be followed up.

Standaert provides an update for *CHES* which was moved to Leuven, Belgium. The main change is that this will be run as a dual-track conference.

Yang explains that *Asiacrypt* is on track. There is a possibility that there will be travel restrictions depending on the COVID situation in Taipei, Taiwan. The President suggests to consider the penalties for the IACR when we decide to go hybrid and keep an eye on when we need to decide this exactly.

Hale updates the Board that the dates for *Crypto '23* have been set to August 21-24, 2023. Malkin explains that there are some some uncertainties related to venue of *TCC*. This is investigated and will be followed up.

2.2. **Eurocrypt 2023 Search update.** The President announces that a venue for *Eurocrypt '23* has been found: this will be organized by Stehlé in Lyon, France late April 2023. The President is already looking into the selection for *Eurocrypt* 2024 and 2025.

3. Topics

3.1. **Test-of-Time Award 2022 feedback.** The Board received feedback from Smart (chair of the Test-of-Time Selection Committee 2022). Currently, the selection committee in any year includes two members appointed by the Board of Directors, and three program chairs of the current year's IACR general conferences as ex-officio members. However, the program chairs are extremely busy with the conferences and don't have much time for this selection and very little input was received. The suggestion is to consider changing the composition. Yung suggests to look how we run the Fellow Committee. The Presidents suggests that we rethink the composition but parks this topic due to time constraints.

3.2. **Schedule for future votes (2024 PC co-chair selections, New Journal EiC, etc.)** The President explains that we need to start appointing Chairs in the upcoming meetings. As agreed in the previous Board meeting the nominations should be done a week in advance before the meeting where we vote on them. In the next Board meeting we will select the first PC Chair for *Eurocrypt '24*. Bos also recalls that we look for nominations for the EiC(s) for the New Journal.

Action Point **2: Bos** *(no time set)*:
Update the list of potential PC chairs and share this with Board.

3.3. **IACR School Proposal.** The Schools Committee received one proposal after the deadline which has been shared with the Board. After alignment with the President this was not considered as a problem in the current circumstances: the Board agrees. The proposal is to organize IACR-VIASM Summer School on Cryptography to be held in Hanoi, Vietnam. The proposal is discussed in detail and it is noted that the proposal includes well-known speakers (with inclusion and diversity) and a diverse set of advanced topics.

Decision 2 (unanimous)**.** *The Board follows the recommendation by the Schools Committee and decides to fund the IACR-VIASM Summer School on Cryptography to be held in Hanoi, Vietnam for 8000 USD.*

3.4. **Financial update (authorized signers, wise).** The Treasurer explains that we need to update the list of authorized signers for the upcoming conferences.

Decision 3 (unanimous)**.** *BE IT RESOLVED by the Board of Directors of the International Association for Cryptologic Research that individuals be added or removed as authorized signers from the corresponding bank accounts as indicated in the following table:*

Bank Account (Institution, Acct#)	**Add/Remove**	**Name of Authorized Signer**
First Security Bank of WA (FSBWA), Acct #5151084090, IACR Checking	Add	Michel Ferreira Abdalla (President)
FSBWA #5151512750, CRYPTO Checking	Add Add	Allison Bishop (CRYPTO 2022 GC) Michel Ferreira Abdalla (President)
FSBWA #5151305620, CHES Checking	Remove Remove Remove Add	Vincent Mooney (CHES 2019 GC) Yunsi (Vivien) Fei (CHES 2019 GC) Patrick Schaumont (CHES 2019 GC) Michel Ferreira Abdalla (President)
FSBWA #5151512790, TCC Checking	Remove Add Add	Alessandra Scafuro (TCC 2021 GC) David Cash (TCC 2022 GC) Michel Ferreira Abdalla (President)
Fidelity Investments #Z40115311	Add	Michel Ferreira Abdalla (President)

LaMacchia also updates the Board that due to the creation of the IACR subsidiary we again have a Wise account approved. This means we pay only 0.5 percent instead of 3.0 percent currency conversion fees. The President thanks LaMacchia for all his work.

3.5. **FSE Statement.** During *FSE* a statement by the FSE Steering Committee was discussed and presented. The main message is the same as they expressed before and discussed in the Board: they see that the creation of a New Journal would result in a publication landscape which is very confusing. They suggest instead to limit the innovation in publications for this new journal to the areas not covered by FSE and CHES.

The statement is discussed by the Board. Bos agrees that the New Journal Committee should communicate better with the various Steering Committees. It was unfortunate that this statement was not discussed with the New Journal Committee. Yung and Bos explain that limiting topic areas from the journal is absurd: this is against the spirit of the New Journal. McCurley suggests to communicate this at other venues and ask for feedback: in April there will be *RWC*: the largest IACR event. He suggests to present the New Journal proposal there and ask for feedback, he agrees that limiting the topic areas is absurd. Yung explains that our field has grown, another journal adds something new. In the end the Membership should decide if we should create this (or not).

Preneel asks the question where the IACR sees itself in 10 years with respect to publishing. LaMacchia seconds this question: the IACR needs a long-term publication strategy. The President suggests that we all think about this question and come back to this.

4. Closing Matters

The President closes the meeting at 00h06 CET.