

MINUTES IACR BOARD MEETING *VIRTUAL-06 2023*

15 JUNE 2023

1. OPENING MATTERS

1.1. Welcome, roll of attendees, identification of proxies. At 14:05 UTC 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 the following proxies: Lysyanskaya holds Bishop's proxy (when absent), Halevi holds Yung's proxy (when absent), Poettering holds Hesse's proxy (when absent).

1.1.1. *Roll of Attendees.*

Attendees (Elected). Michel Abdalla (President 2023-2025); Brian LaMacchia (Treasurer 2023-2025); Benjamin Wesolowski (Secretary 2023-2025); Masayuki Abe (Director 2021-2023); Jian Guo (Director 2022-2024); Shai Halevi (Director 2023-2025); Tancrede Lepoint (Director 2021-2023, *Crypto 2024* General Chair (2023-2024)); Anna Lysyanskaya (Director 2022-2024); Bart Preneel (Director 2023-2025, *FSE* Steering Committee, Program Chair Contact); Peter Schwabe (Director 2023-2025); Bo-Yin Yang (Director 2022-2024); Moti Yung (Director 2021-2023, *PKC* Steering Committee);

Attendees (Appointed). Foteini Baldimtsi (Communications Secretary 2023-2025); Britta Hale (*Crypto 2023* General Chair (2022-2023)); Julia Hesse (*Eurocrypt 2024* General Chair (2023-2024)); Bertram Poettering (Membership Secretary 2023-2025); Vincent Rijmen (Journal of Cryptology Editor-in-Chief 2021-2023); Bimal Roy (*Asiacrypt 2024* General Chair 2023-2024); Damien Stehlé (*Eurocrypt 2023* General Chair (2022-2023)); Fangguo Zhang (*Asiacrypt 2023* General Chair (2022-2023));

Attendees (Representatives and Others). Tal Malkin (*TCC* Steering Committee);

Absentees (Elected). Allison Bishop (Vice President 2023-2025);

Absentees (Representatives and Others). Mitsuru Matsui (*Asiacrypt* Steering Committee); Kevin McCurley (Database Administrator); 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. The President calls for a vote to approve the minutes.

Decision 1 (unanimous). *The Board approves the Minutes of the IACR Board Meeting Virtual-04 2023.*

2. CONFERENCES

2.1. Update on conferences. Hale provides an update on *Crypto*, stating that the budget has been approved and good progress has been made with vendors. 23 invitation letters have been sent and 43 students have applied for stipends. The documentary crew will be allowed to film the talks, which are public anyway. Lysyanskaya mentions that 124 papers have been accepted, which is a record number. All has been sent to Springer. As an experiment, it was checked if the tex files compiled, and the vast majority did. The program is almost ready, and it is planned to have 30-minute breaks and long lunch breaks. Remote presentations will be allowed on a case-by-case basis under extenuating circumstances.

Schwabe provides an update on *CHES*: there are new sponsors, and 79 papers have been accepted. Concern has been expressed regarding the status of the event *TASER*. It is presented as an affiliated event, which are on a separate budget. But it is considered part of *CHES*, and was initiated by the steering committee; in 2022 it was given special treatment, included in the main program alongside the tutorials. This needs to be regularized, maybe by not considering it as an affiliated event.

Malkin gives an update on *TCC*, stating that all is going well. Yang mentions that they are getting ready for visa assistance as soon as results are out.

Zhang updates on *Asiacrypt*: the hotel has been chosen and the contract for the conference venue is being prepared. There has been a record number of submissions. It is possible to have three tracks but the third room is smaller.

2.2. FSE 2024 proposal. The President introduces the next agenda item, which concerns the proposal for *FSE 2024* in Leuven that has been submitted to the board. The main point of discussion revolves around how the finances will be handled, considering the previous issues encountered during *CHES 2022* in Leuven. It is suggested to revise the general chair guidelines, as opening bank accounts in the name of the IACR in Europe has become increasingly difficult. Going through KU Leuven for handling funds is associated with an administration fee. It is clarified that this fee is more of a general service fee, providing access to facilities and other services. There is a debate regarding whether this arrangement offers VAT advantages.

Halevi suggests the potential hiring of a long-term service in Europe to handle such financial matters. The President proposes updating the guidelines to encourage proposals to include detailed plans for handling finances. It is mentioned that the current FSE proposal appears satisfactory overall, and the President proposes to vote under the assumption that a satisfactory contract will be signed with KU Leuven.

Decision 2 (unanimous). *The proposal to host FSE 2024 in Leuven is approved.*

3. APPOINTMENTS

3.1. Asiacrypt 2025 Program Chair. The President reminds the attendees about the need to nominate two program chairs for Asiacrypt 2025. It is mentioned that six candidates were nominated, and one of them is present in the meeting. The nominee leaves the meeting for the duration of the vote. The candidates are presented by the board members who nominated them, then the President calls for a vote to select the first Program Chair.

Decision 3. *Bo-Yin Yang is appointed Asiacrypt 2025 Program Chair. [Yang has since accepted.]*

After a brief discussion on the remaining candidates and their complementarity with Yang, the President calls for a vote to select the second Program Chair.

Decision 4. *Goichiro Hanaoka is appointed Asiacrypt 2025 Program Chair. [Hanaoka has since accepted.]*

4. TOPICS

4.1. Recent scam attempts. The President addresses the issue of recent scam attempts, informing the attendees that many board members and possibly other IACR members have received emails impersonating the President. These emails first ask for help and then request money if a response is received.

To address this issue, it is suggested to send a warning to anyone who has an email address published on the IACR website. Additionally, it is proposed to include a warning in the welcome email sent to new board members. The attendees are reminded to exercise caution, as it is now even possible to receive phone calls that sound like they are from another board member.

4.2. Proposal for improving Diversity, Equity, and Inclusion. The President introduces the next agenda item, which concerns the document *On Creating a More Inclusive and Supporting Community* which was shared with the board, and includes ideas that could be implemented by the IACR.

It is noted that not all ideas presented in the document fall under the purview of the IACR; some are the responsibility of universities.

The first idea discussed concerns easing the process of obtaining visas for conferences, via an automated template to generate visa letters. Schwabe raises a concern about the potential abuse by visa scammers of an automated platform. Stehlé adds that visa issues are also caused by delays, as notifications often arrive late. Two waves of demands are observed: one at acceptance notification and another at the publication of the program.

LaMacchia brings up the third idea mentioned in the document, which relates to financial support for traveling to conferences. It is highlighted that offering financial support is already mentioned in the general chair guidelines, but the general chair has flexibility in how it is implemented.

The President concludes that these are all valuable discussions to have at the next strategic meeting.

5. CLOSING MATTERS

Abdalla closes the meeting officially at 15:56 UTC.