

MINUTES IACR BOARD MEETING *VIRTUAL-02 2023*

21 FEBRUARY 2023

1. OPENING MATTERS

1.1. Welcome, roll of attendees, identification of proxies. At 15h04 UTC Abdalla opens the meeting and briefly goes around for an introductory round, confirming attendees and establishing who is holding proxies. There are 20 full time attendees with the following proxies: Bishop holds Lysyanskaya proxy (when absent), Yang holds Schwabe's proxy (when absent), Poettering holds Hesse's proxy (when absent).

1.1.1. *Roll of Attendees.*

Attendees (Elected). Michel Abdalla (President 2023-2025); Allison Bishop (Vice President 2023-2025); Benjamin Wesolowski (Secretary 2023-2025); Brian LaMacchia (Treasurer 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); Damien Stehlé (*Eurocrypt 2023* General Chair (2022-2023)); Fangguo Zhang (*Asiacrypt 2023* General Chair (2022-2023));

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

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. Preneel proposes a modification: the Vice President is only expected to chair the Audit and Ethics committees, not the Schools committee. The President calls for a vote to approve the minutes, subject to this modification.

Decision 1 (unanimous). *The Board approves the Minutes of the IACR Board Meeting Virtual-01 '23.*

2. CONFERENCES

2.1. Update on upcoming conferences. Preneel reports on the organisation of *FSE*, and briefly discusses the budget (mentioning the possible impact of the dual location). Schwabe reports on *RWC*: the list of accepted talks is online, and registrations are open. Stehlé reports on the organisation of *Eurocrypt*: technique and food contracts are signed, and the final budget has been submitted for approval. The registration fee will certainly be slightly lower than the 2022 edition, despite inflation, thanks to the sponsors. Yung reports that 50 papers have been accepted at *PKC*. Hale reports on the organisation of *Crypto*: the main contract is signed, and they are drafting agendas for either dual or triple tracks. Schwabe reports that sponsors for *CHES* are trickling in. Malkin reports that the organisation of *TCC* is moving along well. Zhang reports that *Asiacrypt* can probably be held in person.

2.2. Update on Eurocrypt venues. Future venues for Eurocrypt are briefly discussed: after *Eurocrypt 2024* in Zurich, proposals are being drafted up to 2026.

2.3. Asiacrypt 2024 and 2025 proposals. Two proposals for *Asiacrypt* are presented: a proposal to hold *Asiacrypt 2024* in Kolkata, India, and a proposal for *Asiacrypt 2025* in Melbourne, Australia.

The *Asiacrypt 2025* proposal presents two possibilities for the hotel, and Preneel raises the point that the vote should concern a specific option. Bishop notes that the proposal does favour one of the hotels (more expensive, but higher buffer for more people attending, and better location). The board is invited to review the detailed proposals, and send any feedback by email. A vote will soon be called.

3. APPOINTMENTS

3.1. Program Chair 2025 selection schedule. The president proposes a schedule for the selection of program chairs for the 2025 General Conferences. Program chairs would be selected for Eurocrypt, Crypto and Asiacrypt in the Board Meetings of March, April, and May respectively. For each General Conference, both program chairs would be selected during the same meeting, and invitations sent simultaneously. This schedule is approved by the board.

3.2. CiC Editor-in-Chief candidates (questions for the candidates). The President recalls that we need to select the second Editor-in-Chief for the IACR Communications in Cryptology journal. The board is invited to discuss and agree on a list of questions for the candidates. Several ideas are proposed. The positioning of the new journal is of particular focus, notably with respect to Area Conferences, and the expected level. The time commitment is also discussed: the intensity of the workload, and the duration of a term.

Action Point 1: Wesolowski (<i>Soon after the meeting</i>): Draft the list of questions to candidates.
--

Once the list is drafted, further adjustments will be discussed via email. The questions will be sent to the candidates before the next Board Meeting.

4. TOPICS

4.1. Date / venue for next IACR strategic meeting. The President notes that in addition to the monthly virtual Board Meetings, it is desirable to hold at least one physical meeting per year. He suggests to meet at *Eurocrypt* this year, in Lyon. A few members express their approval, and confirm they will indeed be present at *Eurocrypt 2023*.

That meeting will not replace the April virtual meeting. It will be a strategic meeting, that may last a full day. The nature of the meeting and its agenda is briefly discussed. Halevi mentions issues that need revisiting and decisions that need to be acted on (concerning, for instance, the edition of conference proceedings). Yung underlines the *strategic* nature of the meeting: it is the place for long term and large scale discussions, concerning the whole field and the next few decades.

The date of the meeting is then discussed. Stehlé says that the Tuesday afternoon of *Eurocrypt 2023* is free. Lysyanskaya and Yung say that these long meetings have previously been held on the Sunday preceding the event. Hesse notes that it conflicts with the *Eurocrypt* workshops. The president calls for a vote.

Decision 2. *The next IACR strategic meeting will be held in Lyon, France on Sunday, March 23, 2023.*

5. CLOSING MATTERS

Abdalla closes the meeting officially at 16h10 UTC.