

MINUTES IACR BOARD MEETING *VIRTUAL-03 2023*

22 MARCH 2023

1. OPENING MATTERS

1.1. Welcome, roll of attendees, identification of proxies. At 14h04 UTC Bishop opens the meeting and briefly goes around for an introductory round. There are 21 full time attendees with the following proxies: Halevi holds Lepoint's proxy, and Schwabe holds Yang'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); Masayuki Abe (Director 2021-2023); Jian Guo (Director 2022-2024); Shai Halevi (Director 2023-2025); 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));

Absentees (Elected). Brian LaMacchia (Treasurer 2023-2025); Tancrede Lepoint (Director 2021-2023, *Crypto 2024* General Chair (2023-2024));

Absentees (Appointed). Bimal Roy (*Asiacrypt 2024* General Chair (2023-2024));

Absentees (Representatives and Others). Tal Malkin (*TCC* Steering Committee); 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 Vice President thanks the Secretary for the completion of the minutes which have been shared before the current Board Meeting. The Vice President calls for a vote to approve the minutes.

Decision 1 (unanimous). *The Board approves the Minutes of the IACR Board Meeting Virtual-02 '23.*

The President arrives and reviews the agenda.

2. CONFERENCES

2.1. Update on upcoming conferences. Preneel reports on the organisation of *FSE*: attendance is good in both venues (Kobe and Beijing). Abdalla mentions that there was a problem with the banking setup; it seems to be resolved, but we may want to investigate what went wrong. Schwabe reports on *RWC*: the program is online, and 625 people have registered, approaching the capacity of the venue (650). On-site registration may not be guaranteed. Stehlé reports on the organisation of *Eurocrypt*: registration has opened, with already 263 attendees. Yung reports on *PKC*: registration is about to open, after a delay due to a correction of the budget. The list of accepted papers is out, and the proceedings are being worked on.

Schwabe reports on *CHES*: they are expecting about 85 papers. The event will last 3.5 or 4 days depending on the exact numbers. The following question has been raised by the steering committee: is it the prerogative of the steering committee to decide "how hybrid" (in-person and virtual) the event may be? The President answers that yes, it is. A discussion follows on which of the in-person or hybrid format is best. It is noted that the hybrid format degrades the in-person experience. Also, if authors are not asked to present in-person, employers may require their authors to present remotely. Bishop notes that attendance has increased dramatically with online events, hinting at the number of people who cannot attend traditional conferences (Schwabe responds by asking whether we have a reliable way to measure online attendance: online registration has often been free, so registration statistics may not reflect actual attendance). Two mitigations are mentioned: Halevi mentions colocation of events (like *FSE*

2023), which facilitates travel; Yung mentions the fact that talks are recorded and published, which allows free online access to the scientific content of conferences.

Hale reports on the organisation of *Crypto*: sponsorship is lower than expected, and the number of submissions hits a record high.

3. TOPICS

3.1. Limits on number of submissions and number of pages. Preneel brings two questions to the attention of the Board: (1) should the limit on the number of submissions by program committee members be increased from 2 to 3 and (2) should the page limit for submissions be decreased?

3.1.1. *Limit on the number of submissions by program committee members.* The motivation to relax the limit is that the total number of submissions keeps increasing. Lysyanskaya says that it would incentivise more people to join the program committee (currently, the acceptance rate is often around 50%). Yung notes that the limit used to be stricter: either two papers with student co-authors, or one paper without. Originally, the limit may have stemmed from a feeling in the 90's that program committee members would take too many slots in the program. Preneel asks whether we could do statistics on what is actually happening nowadays.

No definitive conclusion is reached, but the discussion leans in favour of the increase.

3.1.2. *Limit on the number of pages.* Regarding the page limit, the matter has been discussed during the Virtual-01 2023 Board Meeting. Abdalla summarises that we do not recommend a reduction of the page limit. It is however recommended to remove the references from the limit.

3.2. Next IACR strategic meeting preparation. The President recalls that a strategic meeting will be held in Lyon, during *Eurocrypt 2023*. He calls for a volunteer to collect the list of topics to be discussed at the strategic meeting. Bishop volunteers.

Action Point 1: **Bishop** (*no time set*):
Collect the list of topics for the strategic meeting.

It is then decided that the strategic meeting will start on Sunday, April 23, after lunchtime.

4. APPOINTMENTS

4.1. CiC Editor-in-Chief. The President recalls that we need to select the second Editor-in-Chief for the IACR Communications in Cryptology journal. Five candidates were previously approved by the board. Three remain, due to two withdrawals. They have prepared responses to the list of questions prepared during the last Board Meeting; these were sent to Board members ahead of the present meeting. The President calls for a vote.

Decision 2. *Andreas Hülsing is appointed co-Editor-in-Chief for the IACR Communications in Cryptology journal. [Hülsing has since accepted.]*

4.2. Eurocrypt 2025 Program Chair. The President recalls that we need to select the two Program Chairs for *Eurocrypt 2025*. Five people were nominated. Each candidate is presented by the board member who nominated them, and the President calls for a vote to select the first Program Chair.

Decision 3. *Pierre-Alain Fouque is appointed Eurocrypt 2025 Program Chair. [Fouque has since accepted.]*

The President calls for a vote to select the second Program Chair.

Decision 4. *The second Eurocrypt 2025 Program Chair is selected. [the candidate has since declined.]*

5. CLOSING MATTERS

Abdalla closes the meeting officially at 15h29 UTC.