

MINUTES IACR BOARD MEETING *VIRTUAL-04 2023*

18 APRIL 2023

1. OPENING MATTERS

1.1. Welcome, roll of attendees, identification of proxies. At 21h05 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: Abdalla holds Bishop's proxy (when absent), Preneel holds Lepoint's proxy (when absent), Halevi holds Lysyanskaya's proxy, Yang holds Schwabe's proxy, Preneel holds Rijmen's proxy, Abdalla holds Stehlé's proxy (when absent).

1.1.1. *Roll of Attendees.*

Attendees (Elected). Michel Abdalla (President 2023-2025); Allison Bishop (Vice 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); Tancrède Lepoint (Director 2021-2023, *Crypto 2024* General Chair (2023-2024)); Bart Preneel (Director 2023-2025, *FSE* Steering Committee, Program Chair Contact); 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); 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 (Elected). Anna Lysyanskaya (Director 2022-2024); Peter Schwabe (Director 2023-2025);

Absentees (Appointed). Vincent Rijmen (Journal of Cryptology Editor-in-Chief 2021-2023); Bimal Roy (*Asiacrypt 2024* General Chair 2023-2024);

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. The President calls for a vote to approve the minutes.

Decision 1 (unanimous). *The Board approves the Minutes of the IACR Board Meeting Virtual-03 2023.*

2. CONFERENCES

2.1. Update on conferences. *FSE* has just happened, all went well. The Treasurer reports that all looks okay on the financial side, all payments are made. Attendance broke the *FSE* record. *RWC* has also ended; it sold out and all went well.

Yung reports on the organisation of *PKC*: all is going according to plan. Abdalla notes that the projected attendance is lower than expected, and the early registration deadline has been pushed. The Treasurer notes that low attendance is likely to be an issue for the budget, due to the blocked hotel rooms. It is noted that such accommodation agreements can be a risk for the budget of smaller conferences. Stehlé reports on *Eurocrypt*: registration is approaching the capacity of the venue (715 participants). They are discussing how to freeze the registration page.

Hale reports on *Crypto*: the first sponsor is in. A small company has reached out about the possibility to film some talks for a documentary. Bishop notes that it may be hard to control what they film (crowd shots?). Brian says that it may require having the attendees all agree to be filmed in the registration form; that has never been done and may not be a good idea. If possible, a solution would be to only allow them to film content that is made public anyway: only the talks (which are published on the IACR Youtube channel), with the speakers'

authorisation. Otherwise, they could simply use the content from the Youtube channel, which is published under the IACR creative commons licence.

Zhang reports on *Asiacrypt*: the program committee is being selected, and the call for paper will be published soon. Malkin reports on *TCC*: all is going well, the committee is ready, and the submission deadline will be announced soon.

2.2. Awards and IACR Fellows. The President reports on the Test-of-Time award. The winners are notified two months ahead of the conference. The public announcements are made one by one, for each awardee to get proper recognition. The President adds that the 2023 IACR fellows will be announced in the coming days.

3. TOPICS

3.1. Upcoming strategic meeting. The board will hold a strategic meeting in Lyon on April 23, from 2pm to 6pm local time (CEST). Bishop has collected a list of topics for the agenda of the meeting. The following topics have been proposed:

- (1) Publication model (in particular, should IACR move away from Springer?)
- (2) Collocation of conferences (holding two events near each other to reduce travel)
- (3) Policy for hosting conferences in hybrid format (online and on-site)
- (4) Policy on generative AI for submissions
- (5) Planning future IT support for the association (which currently lies mostly on the shoulders of Kevin McCurley)

On the topic of publication, McCurley underlines the low quality of submitted LaTeX documents, with about 10% of submissions that do not compile. There are plans to automatically check that the server can compile them. About publication models, Gaëten Laurent's *A Proposal for Reorganizing the IACR Publications Landscape* is mentioned. It may be worth inviting him to discuss the matter at the strategic meeting.

3.2. Discussion on double and triple tracks. The President recalls the matter at hand: the General Conferences are becoming larger (in number of submissions, number of accepted papers, and attendance). They are already hosting two parallel tracks. To accommodate the increasing number of presentations, it may be necessary to organise triple tracks (it is already the case for *Eurocrypt 2023*), but that increases the costs.

Hesse reports on the impact of triple tracks on the organisation of *Eurocrypt 2024* in Zurich: going from double to triple costs an additional 67,000 USD, according to the current planning. Triple tracks may reduce the number of lunches (thanks to a free afternoon), which cost 25,000 USD each. However, if lunches are cancelled, the venue may increase the rent to compensate.

The current projected registration fee is at 1000 USD (for an expected attendance at 550, and with the current CHF rate).

Stehlé reports that for *Eurocrypt 2023*, the triple tracks have increased the budget by 50,000 USD.

Halevi says we may have no choice but accept that our conferences are getting bigger. Yung adds that triple tracks may indeed be necessary in order to maintain the acceptance rate. Stehlé agrees but insists that we should strive to keep prices low: there are already complaints against the *Eurocrypt 2023* fee of 725 USD. Maybe online attendance should not be free anymore, and maybe the student price should be higher than 50% of the regular price (at *Eurocrypt 2023*, each new student costs money, as the fee does not cover the variable cost per delegate).

LaMacchia adds that we are heading to a point where it is going to be difficult to stay an all-volunteer organisation. We may soon need the help of professional organisers.

Preneel asks whether costs could be reduced with lower quality catering. Hesse answers that venues enforce a lower bound on catering, so we cannot cut these costs too low.

4. APPOINTMENTS

4.1. Eurocrypt 2025 Program Chair. The President recalls that Pierre-Alain Fouque has accepted his appointment as Program Chair for *Eurocrypt 2025*, but the second appointee has declined, so the Board needs to appoint another one. Five people have been nominated. Each candidate is presented by the board member who nominated them, and the President calls for a vote to select the second Program Chair.

Decision 2. *Serge Fehr is appointed Eurocrypt 2025 Program Chair. [Fehr has since accepted.]*

The board agrees that if Fehr declines, the nomination goes to the runner-up.

4.2. Eurocrypt 2025 Program Chair. The President recalls that we need to select the two Program Chairs for *Crypto 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. *Yael Kalai is appointed Crypto 2025 Program Chair. [Kalai has since accepted.]*

The Board briefly discusses the complementarity of other nominees with Kalai's profile. The President calls for a vote to select the second Program Chair.

Decision 4. *Seny Kemara is appointed Crypto 2025 Program Chair. [Kemara has since accepted.]*

5. CLOSING MATTERS

Abdalla closes the meeting officially at 22h56 UTC.