

# MINUTES IACR BOARD MEETING *VIRTUAL-05 2024*

7 MAY 2024

## 1. OPENING MATTERS

**1.1. Welcome, roll of attendees, identification of proxies.** At 14:03 UTC the President 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, Yang holds Guo's proxy, Rodríguez-Henríquez holds Naya-Plasencia's proxy, Halevi holds Yung's proxy, Abdalla holds Fiore'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); Shai Halevi (Director 2023-2025); Anna Lysyanskaya (Director 2022-2024); Bart Preneel (Director 2023-2025, Program Chair Contact); Francisco Rodríguez-Henríquez (Director 2024-2026); Peter Schwabe (Director 2023-2025); Bo-Yin Yang (Director 2022-2024);

*Attendees* (Appointed). Dario Fiore (Eurocrypt 2025 General Chair (2024-2025)); Julia Hesse (*Eurocrypt 2024* General Chair (2023-2024)); Tancrède Lepoint (*Crypto 2024* General Chair (2023-2024)); Vincent Rijmen (Journal of Cryptology Editor-in-Chief 2024-2026); Bertram Poettering (Membership Secretary 2023-2025);

*Attendees* (Representatives and Others). Kevin McCurley (Database Administrator);

*Absentees* (Elected). Allison Bishop (Vice President 2023-2025); Jian Guo (Director 2022-2024); María Naya-Plasencia (Director 2024-2026); Moti Yung (Director 2021-2023, *PKC* Steering Committee);

*Absentees* (Appointed). Foteini Baldimtsi (Communications Secretary 2023-2025); Joseph Liu (*Asiacrypt 2025* General Chair (2024-2025)); Bimal Roy (*Asiacrypt 2024* General Chair 2023-2024);

*Absentees* (Representatives and Others). Hilarie Orman (Archivist); Tal Rabin (Code-of-conduct Liaison); Yu Yu (Webmaster);

## 2. CONFERENCES

**2.1. Update on upcoming conferences.** Hesse reports on *Eurocrypt 2024*. There are now 650 registrations. She raises a concern about the refund policy: it states that last minute cancellation will not be refunded. Because of this strict policy, and the ongoing conflict in the middle east, researchers from Israel have refrained from registering. The President responds that we are usually flexible with the refund policy in such exceptional circumstances. General Chairs can overrule this policy when they believe it justified. Yang adds that for *TCC* in Taiwan, they issued a statement saying they would show flexibility for any person affected by the conflict.

Lepoint reports on *Crypto 2024*. Notifications for accepted papers have been sent. There will be 135 presentation slots, each of 20 minutes (instead of 25). Requests for invitation letters are coming in. Abdalla suggests that we could automate invitation letters for accepted papers.

## 3. TOPICS

**3.1. Items for the upcoming strategic meeting at Eurocrypt.** The President recalls that we will soon meet for the strategic meeting at *Eurocrypt 2024*. In preparation, we are compiling a list of items to be discussed. Two topics are submitted:

- The publication and conference model; a working group has already been formed to investigate the matter.
- Requirements for the selection of Program Chairs. We have been postponing the selection of the *Crypto 2026* and *Asiacrypt 2026* Program Chairs to first settle this question.

The President calls for the Board members to send further items by email before *Eurocrypt*.

Poettering recalls that the strategic meeting will be hosted at IBM. Lysyanskaya notes that it is far from ETH, where the workshops will take place. She asks whether it is possible to organize the meeting at ETH instead. Hesse responds that it is not possible during the weekend. We may try to host it at Google or Dfinity, both much closer to ETH than IBM.

Regarding Item 3.1 (the publication and conference model), McCurley suggests gathering information from communities experiencing similar scaling issues. The working group has already discussed this with Carmela Troncoso about the situation in the security community (regarding the future format of USENIX, see <https://github.com/USENIX-Security-2025/conference-format>). We could also ask communities outside computer science.

McCurley notes that the discussion on publication models is related to other matters, like setting incentives for reviewing.

**3.2. IACR Statement On the War in Gaza.** The President recalls that the amendment to the IACR Statement On the War in Gaza was approved on April 29 in a vote by email. The following text will be added to the original one, clearly presented as an addendum: *“The IACR is further horrified by the devastation and loss of life suffered by civilians in Gaza in the ongoing war, and the continued immense suffering in Gaza, Israel, and elsewhere”*. The title will be changed to *“IACR Statement On the War in Gaza”*, and a note recording the original title will be added.

#### 4. CLOSING MATTERS

The President informs the Board that the venue contract for *Eurocrypt 2026* in Rome has just been signed. Two proposals for *Eurocrypt 2027* are being prepared, and the Board will review them in the coming months.

The President closes the meeting officially at 15:16 UTC.