MINUTES IACR BOARD MEETING *VIRTUAL-07 2024*

24 JULY 2024

1. Opening Matters

1.1. **Welcome, roll of attendees, identification of proxies.** At 14:04 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: Yang holds LaMacchia's proxy, Halevi holds Lysyanskaya's proxy (when absent), Schwabe holds Yang's proxy (when absent), Wesolowski holds Poettering'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); Jian Guo (Director 2022-2024); Shai Halevi (Director 2023-2025); Anna Lysyanskaya (Director 2022-2024); María Naya-Plasencia (Director 2024-2026); Bart Preneel (Director 2023-2025, Program Chair Contact); Francisco Rodríguez-Henríquez (Director 2024-2026); Peter Schwabe (Director 2023-2025, *CHES* Steering Committee); Bo-Yin Yang (Director 2022-2024);

Attendees (Appointed). Dario Fiore (Eurocrypt 2025 General Chair (2024-2025)); Tancrède Lepoint (*Crypto 2024* General Chair (2023-2024)); Bertram Poettering (Membership Secretary 2023-2025);

Attendees (Representatives and Others). Gregor Leander (*FSE* Steering Committee);

Absentees (Elected). Brian LaMacchia (Treasurer 2023-2025, *RWC* Steering Committee); Moti Yung (Director 2021-2023, *PKC* Steering Committee);

Absentees (Appointed). Foteini Baldimtsi (Communications Secretary 2023-2025); Julia Hesse (*Eurocrypt 2024* General Chair (2023-2024)); Joseph Liu (Asiacrypt 2025 General Chair (2024-2025)); Vincent Rijmen (Journal of Cryptology Editor-in-Chief 2024-2026); Bimal Roy (*Asiacrypt 2024* General Chair 2023-2024);

Absentees (Representatives and Others). Tal Malkin (TCC Steering Committee Representative); Mitsuru Matsui (*Asiacrypt* Steering Committee); Kevin McCurley (Database Administrator); Hilarie Orman (Archivist); Tal Rabin (Code-of-conduct Liaison); Yu Yu (Webmaster);

2. Conferences

2.1. **Eurocrypt 2025 Update.** Dario Fiore presents the first item in the agenda. The organizers are facing a challenge with the organization of the affiliated events at *Eurocrypt 2025* in Madrid. Affiliated events have been growing in the recent years: up to 343 registered participants in 2023, with 40 to 70 participants per workshop, then up to 442 participants in 2024, with up to 120 participants in a single workshop (according to non-committing preferences expressed at registration). The growth in both the total number of participants and the number per workshop presents a challenge.

The venue in Madrid has 6 rooms with 60 to 70 seats, and one room with 100 seats (for a total of 490 seats). Moreover, the indoor lunch area only fits 350 people; the outdoor area can accommodate an additional 150 people. These numbers are tight, in light of the recent growth. The loose registration procedure (registration per day, during which one can attend any workshop) makes it hard to predict the distribution of participants.

The General Co-Chairs have a few potential solutions in mind:

- Enforcing a cap on the number of workshop registrations. If participants are allowed to attend any of the workshops, the cap would need to be substantially below maximum capacity.
- Enforcing the choice of a single workshop, with the possibility of a cap per workshop.
- Finding a different venue. For instance, UCM has more rooms and larger rooms. However, it is possibly more expensive and the organizers are not from that university.

Fiore asks the Board for feedback on the issue and the proposed solutions, prompting a discussion.

- Schwabe notes that if we do not provide lunches, the indoor limit of 350 is lifted. Relying on outdoor space is risky in case of bad weather.

- Preneel points out that if we ask participants to register for one specific workshop, it would be hard to make sure they commit to this choice. We would rely on good communication and good faith. In view of this it may be better to move one or more larger workshops to another venue, that could also be a hotel.
- Halevi says that the growth of affiliated events is a mark of success, and people see value in them. Going for a bigger venue may be the best solution.
- Schwabe suggests that an Affiliate Events Chair from UCM could be nominated. Fiore responds that it would be good, but there are no members from the IACR community at UCM.

3. Topics

3.1. **Selection of Program Chairs for Asiacrypt 2026.** The President recalls that we need to select the two Program Chairs for *Asiacrypt 2026*. 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 1. *A first candidate is selected for Asiacrypt 2026 Program Chair. [The candidate has since rejected the appointment.]*

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

Decision 2. *Naofumi Homma is appointed Asiacrypt 2026 Program Chair. [Homma has since accepted.]*

3.2. **Efforts to update our general policies and documentation.** Bishop introduces the last item in the agenda. She has been working towards updating and syncing up the IACR general policies and documentation. She presents slides (published with the present minutes) listing her findings and recommendations: merging redundant documents, resolving inconsistencies, or revising debatable policies. A discussion ensues.

- Bishop has pointed out some inconsistencies across the policies of our several publication venues, and has suggested that we resolve them and merge the documents. Schwabe explains that some of the statements in the policies of *Transactions on Symmetric Cryptology* (ToSC) or *IACR Transactions on Cryptographic Hardware and Embedded Systems* (TCHES) are necessary for these publications to be indexed as journals. Bishop expects that such constraints should not be an obstacle for creating either a unified policy (with small specificities carved out) or a general-purpose policy template.
- The Secretary says that he is looking into an update of the IACR bylaws, which currently do not acknowledge the existence of the new journal *IACR Communications in Cryptology* (CiC). He recalls that updating the bylaws is more complex than updating policies. An amendment to the bylaws requires ratification by a majority of the ballots cast in a referendum to the IACR members.

4. Closing Matters

The President closes the meeting officially at 15:25 UTC.