MINUTES IACR BOARD MEETING *VIRTUAL-03 2024*

14 MARCH 2024

1. Opening Matters

1.1. **Welcome, roll of attendees, identification of proxies.** At 21:10 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: Halevi holds Lysyanskaya's proxy (when absent), Leander holds Naya-Plasencia's proxy (when absent), Abdalla holds Fiore's proxy , Preneel holds Rijmen's proxy.

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); 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); 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); Julia Hesse (*Eurocrypt 2024* General Chair (2023-2024)); Tancrède Lepoint (*Crypto 2024* General Chair (2023-2024)); Joseph Liu (Asiacrypt 2025 General Chair (2024-2025)); Bertram Poettering (Membership Secretary 2023-2025);

Attendees (Representatives and Others). Gregor Leander (*FSE* Steering Committee); Kevin McCurley (Database Administrator);

Absentees (Elected). Francisco Rodríguez-Henríquez (Director 2024-2026);

Absentees (Appointed). Dario Fiore (Eurocrypt 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). Hilarie Orman (Archivist); 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 of the previous meeting.

Decision 1. *The Board approves the Minutes of the IACR Board Meeting Virtual-02 2024.*

The President calls for a vote to approve the minutes of the *Crypto 2023 Strategic Meeting*.

Decision 2. *The Board approves the Minutes of the IACR Crypto 2023 strategic meeting.*

2. Update on conferences

Leander reports on *FSE 2024*. The conference happens in two weeks, in Leuven. There are currently 140 registered participants — less than last year, which was a record.

LaMacchia reports on *RWC 2024*, also happening in two weeks. Registrations are at 474, which is lower than expected. Organisers are planning a poll to understand (was the program announced too late?).

Hesse reports on *Eurocrypt 2024*. The program is online, and the registrations are about to open. It is noted that some hotel deals have already expired.

Yung reports on *PKC 2024*. The program is online, registrations are open.

Lepoint reports on *Crypto 2024*. The venue, UCSB, is about to increase many of the prices by 55%. It is not clear yet what will be impacted (possibly the per-hour cost of labor, or the facilities) and when (some this year, the rest next year). On another matter, the submission deadline for affiliated events is tomorrow. For the moment, the number of submissions is low. Finally, requests for invitation letters are coming in, and some are also asking for a proof of registration. This is problematic since registrations are not open yet, and the final price is not yet determined. It is possible for participants to pay ahead an estimate of the final price; the General Chair can then issue a registration token. There is no streamlined mechanism to do this: we should implement a better system.

Schwabe reports on *CHES*. The organisation of *CHES 2024* is progressing well. The proposal for *CHES 2025* should soon be the object of a vote.

3. TOPICS

3.1. **IACR Schools Proposals.** Lepoint presents the next topic. Three school proposals have been submitted to the first deadline this year. They have been shared with the Board ahead of this meeting, along with the recommendation of the Schools Committee.

A first general observation is that schools request increasingly high amounts. We usually grant USD 5,000 or 10,000, while some proposals request up to USD 30,000. The Secretary wonders whether the guidelines are not clear enough on the amounts that can be requested. A discussion ensues on how much of its budget the IACR wants to spend for schools (this may be a topic for the next strategic meeting, as part of a discussion on longer term financial goals). The President recalls that the original purpose of the IACR Schools Committee is to help the organisation of schools for places and people that have limited opportunities. Some proposals do not really fall in that category. Another concern is that increasingly many proposals seem to build their budget mostly around IACR support.

Lepoint briefly summarises the three proposals: the *Warsaw Summer School on Post-Quantum Cryptography*, the *IACR Summer School on Security, Privacy, and Verification*, and the *IACR Crypto School on Foundations and Applications of Zero-Knowledge Proofs*. The committee recommends to fund all three schools for the requested amount capped at USD 10,000 The president calls for a vote.

Decision 3 (unanimous)**.** *The Board approves to grant the IACR School status to the three proposals, with the following financial support: USD 10,000 for the Warsaw Summer School on Post-Quantum Cryptography, USD 5,000 for the IACR Summer School on Security, Privacy, and Verification, and USD 10,000 for the IACR Crypto School on Foundations and Applications of Zero-Knowledge Proofs.*

3.2. **Requirements for Program Chairs of General conferences.** The President introduces the next item in the agenda: a discussion on the requirements for the nomination of Program Chairs of General conferences. The current guidelines read: "*Any Voting Board Member may place any individual's name into nomination without restriction. This nomination must be shared with the Board at the latest one week before the voting will take place.*" Should we start establishing some kind of minimal requirements? Past Board discussions on the matter concluded that flexibility is best, and the Board can take decisions on a case-by-case basis. A discussion ensues, raising the following points.

- Any requirements we have should be very inclusive: people in our community are diverse, with various publication practices. Imposing strict requirements on internal IACR service and publications runs a risk of becoming too self-referential, and excluding valuable profiles. Many people in the "cryptologic research" landscape don't have a strong publication record (e.g., in industry). They may still be leaders, and have a relevant view on the value of contributions in cryptography.
- A point is made that publishing is the first currency in research. Being a leader in the community is important for a Program Chair. We may not want to impose a minimum publication requirement, but some kind of publication metric should be attached to the nomination.
- What is the problem we are trying to solve? It is noted that past underperforming Program Chairs would not have been avoided with bibliometric considerations. Bibliometry may still help the Board avoiding questionable appointements. Some Board members expressed their concern that a Program Chair with too few IACR publications could be badly perceived by the community.
- The Board discusses the most important skills of a Program Chair, and organizational skills are emphasized. Candidates should certainly have experience running similar (but smaller) committees. Some Board members expressed the view that people from industry or people who publish regularly in neighboring communities, such as Usenix and CCS (outside of IACR, but still IACR-relevant) should also be considered if they have the required skills.

We are left with the following open question: do we need a better pipeline to select Program Chairs? To identify potential candidates?

Action Point **1:**
Constitute a committee to discuss the question of Program Chair selection.

The committee could prepare for a discussion at the *Eurocrypt 2024 Strategic Meeting*, and possibly draft an update for the nomination guidelines.

3.3. **Selection of Program Chairs for Eurocrypt 2026.** The President recalls that we need to select the two Program Chairs for *Eurocrypt 2026*. Seven 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 4. *Emmanuel Thomé is appointed Eurocrypt 2026 Program Chair. [Thomé has since accepted.]*

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

Decision 5. *Joan Daemen is appointed Eurocrypt 2026 Program Chair. [Daemen has since accepted.]*

4. Closing Matters

The President closes the meeting officially at 23:14 UTC.