MINUTES IACR BOARD MEETING *VIRTUAL-01 2025*

30 JANUARY 2025

1. Opening Matters

1.1. **Welcome, roll of attendees, identification of proxies.** At 15:04 UTC the President opens the meeting and briefly goes around for an introductory round, confirming attendees and establishing who is holding proxies. The President welcomes the two new Board Members Mayank Varia and Edoardo Persichetti.

There are 20 full time attendees with the following proxies: Lysyanskaya holds Varia's proxy (when absent), 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, *RWC* Steering Committee); Benjamin Wesolowski (Secretary 2023-2025); Shai Halevi (Director 2023-2025); Anna Lysyanskaya (Director 2025-2027); María Naya-Plasencia (Director 2024-2026); Bart Preneel (Director 2023-2025, Program Chair Contact); Francisco Rodríguez-Henríquez (Director 2024-2026, *Crypto 2025* General Chair (2024-2025)); Peter Schwabe (Director 2023-2025, *CHES* Steering Committee); Bo-Yin Yang (Director 2025-2027); Moti Yung (Director 2024-2026, *PKC* Steering Committee);

Attendees (Appointed). Dario Fiore (Eurocrypt 2025 General Chair (2024-2025)); Edoardo Persichetti (*Eurocrypt 2026* General Chair (2025-2026)); Mayank Varia (*Crypto 2026* General Chair (2025-2026)); Bertram Poettering (Membership Secretary 2023-2025);

Attendees (Representatives and Others). Masayuki Abe (*Asiacrypt* Steering Committee); Tal Malkin (*TCC* Steering Committee);

Absentees (Elected). Jian Guo (Director 2025-2027);

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

Absentees (Representatives and Others). Gregor Leander (*FSE* Steering Committee); Kevin McCurley (Database Administrator); Hilarie Orman (Archivist); Tal Rabin (Code-of-conduct Liaison); Yu Yu (Webmaster);

2. Update on conferences

Preneel reports on *FSE 2025*. Forty-five papers will be presented. Registrations are open and everything is going well. A proposal for the next edition is in progress.

LaMacchia reports on *RWC 2025*. There will be five co-located events: ZKProof, OSCW, Real-World MPC, FHE.org, and RWPQC. In the future, we might want to have affiliated events instead of co-located events; that would simplify the organization.

Fiore reports on *Eurocrypt 2025*. They are working on the schedule with the Program Chairs. They are planning 20-minute slots for each talk, including questions. The number of talks that could reasonably fit in the program had an impact on the number of accepted submissions. A room has been reserved for the Board meeting in the same venue as the affiliated events.

Yung, Rodríguez-Henríquez and Schwabe briefly report on *PKC 2025*, *Crypto 2025* and *CHES 2025* respectively: everything is going well.

3. Topics

3.1. **Review of open tasks.** The Secretary has compiled a list of open tasks.

- *Updating the Code of Conduct.* Bishop is currently working on an update of the Code of Conduct for our events. A first draft has already been shared with the Board, and feedback is welcome.
- *Sponsorship Committee.* Bishop has been looking for volunteers to form a Sponsorship Committee, tasked with building and maintaining relationships with companies. She, Britta Hale, and Mariana Raykova have volunteered, and she calls for suggestions of people in Europe and Asia.

- *IT Staffing.* Last year, McCurley advised that the IACR begin relying on professional IT services. He has proposed to draft a job description. We will move forward with that proposal.
- *Policy on IACR Statements.* In October 2024, the Board voted to form a working group to draft a policy on IACR Statements. Abdalla volunteers to chair this group. Halevi, Naya-Plasencia, and Lysyanskaya volunteer to join.
- *Publication and conference model.* A working group was formed in 2024 to discuss the publication and conference model for our flagship events. It will continue its activity. Persichetti and Varia volunteer to join the group.
- *Updating the Bylaws.* The Secretary has been working on an update of the IACR Bylaws. Several changes are proposed, mostly to account for the new journal *IACR Communications in Cryptology*. The current draft is open for review by the Board, and comments are welcome.
- *Updating the Program Chair guidelines.* It was proposed to draft a default list of "areas" to be included in the Program Chair guidelines. The goal is to have a balanced and representative list of areas of research in cryptography; each submission to a General Conference is assigned to an area, under the responsibility of an Area Chair. Preneel volunteers to draft a list.
- *Visa issues at Crypto.* In October 2024, the Board discussed the difficulties of obtaining a visa for attending Crypto in the US. Different solutions were mentioned: moving around the Americas, enhancing the capabilities for online attendance, or the organization of a mirror event. This issue will be discussed further in future Board Meetings.
- *Page limit for submissions at our flagship events.* The *Crypto 2025* Program Co-Chairs have proposed to revisit the policy on page limits for submissions to our General Conferences. It is too late for *Crypto 2025*, but can be discussed for future conferences.

3.2. **Additional information on registration form.** Women in Cryptography (WinC) has reached out to the Board with a proposal to add optional questions to the registration form of our conferences. The goal is to collect statistics about the participants of IACR conferences and improve our understanding of the demographics of our community. They propose to add three optional questions: the participant's gender, their level of seniority, and their continent of origin.

The output would consist of privacy-preserving aggregated data for each conference. Such a proposal was already discussed in the past. At the time, it was deemed too complex (particularly to ensure privacy at all levels of the process). However, it is feasible, and the Board will look into the best solutions. The exact questions proposed by WinC have been shared, and the Board will discuss them by email.

4. Closing Matters

The President closes the meeting officially at 16:02 UTC.