MINUTES IACR BOARD MEETING *VIRTUAL-08 2025*

7 AUGUST 2025

1. OPENING MATTERS

1.1. **Welcome, roll of attendees, identification of proxies.** The Vice-President will preside the first part of the meeting. At 14:03 UTC the Vice President opens the meeting and briefly goes around for an introductory round, confirming attendees and establishing who is holding proxies.

There are 20 full time attendees with the following proxies: Yang holds Guo's proxy (when absent), Wesolowski holds Naya-Plasencia's proxy, LaMacchia holds Yang's proxy (when absent), Yang holds Liu'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); Jian Guo (Director 2025-2027); Shai Halevi (Director 2023-2025); Anna Lysyanskaya (Director 2025-2027); 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). Mayank Varia (*Crypto 2026* General Chair (2025-2026)); Bertram Poettering (Membership Secretary 2023-2025);

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

Absentees (Elected). María Naya-Plasencia (Director 2024-2026);

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

Absentees (Representatives and Others). Masayuki Abe (*Asiacrypt* Steering Committee); Gregor Leander (*FSE* Steering Committee); Tal Malkin (*TCC* Steering Committee); Hilarie Orman (Archivist); Tal Rabin (Code-of-conduct Liaison); Yu Yu (Webmaster);

2. UPDATE ON CONFERENCES

Rodríguez-Henríquez reports on the upcoming *Crypto 2025*. Registration numbers are currently lower than expected (196 regular and 167 student registrations). There are 255 registrations for on-campus housing, still slightly below the lower bound contracted with UCSB. A room is reserved for the Strategic Meeting on the Sunday before *Crypto*, which will start at 10am.

Schwabe reports that registration for *CHES 2025* has opened.

LaMacchia provides an update on *Asiacrypt 2025*: Liu sent a request to finalize the registration fee in order to open registrations as soon as possible. Unfortunately, the budget is not yet finalized, and it needs to be confirmed before fixing the registration fee. This matter is currently under discussion. Abdalla notes that opening registrations early would help ease visa applications for attendees. LaMacchia agrees but points out that this also increases currency fluctuation risks (though this risk is often low).

Schwabe reports on *RWC 2026*. For the first time this year, there will be affiliated events (as opposed to independent collocated events). A call for these affiliated events will be issued. Schwabe emphasizes that it should be properly advertised since the community may not expect this change and suggests advertising the call by emailing the Membership. The Board agrees with this proposal.

3. TOPICS

The Vice President proposes to continue the discussion on minimum criteria for Program Chair selection during the upcoming strategic meeting. She then lists the remaining topics for the rest of the meeting.

3.1. **Membership survey about publication and conference issues.** The survey is ready, and we now need to finalize the calendar. We are prepared to open it next Monday. However, the timeline is too short to collect all responses before *Crypto*, and many members (particularly those in Europe) are on vacation. Halevi suggests extending the deadline until mid-September to allow members to return from their vacations and respond. McCurley inquires whether the survey should be open only to current IACR Members or also to individuals who have been members in the past. Varia proposes sending it to all people who have been a member within the past three years.

Bishop submits the following proposal:

- The survey will open next Monday,
- It will be sent to all IACR Members from the last three years,
- A reminder will be sent on September 1st, and
- The survey will close on September 12th.

The Board agrees with this plan.

3.2. **Candidates for the Co-Editor-in-Chief of Communications in Cryptology.** The President reminds the Board that we need to select a new Co-Editor-in-Chief for the journal *IACR Communications in Cryptology*. Several candidates have already been nominated, but more names are needed to ensure a balanced list. After brief discussion, additional nominations are proposed.

These will be formally submitted via email, and the Board will vote on them at the *Crypto 2025 Strategic Meeting*.

3.3. **Initiatives to encourage, facilitate, and or disseminate high quality educational materials about cryptography.** At the *Eurocrypt 2025 Strategic Meeting*, the Board discussed a proposal submitted by Mike Rosulek and Fernando Virdia regarding educational materials about cryptography. While the Board appreciated their ideas, no concrete action was taken. The President proposes engaging with them to determine the next steps.

> Action Point **1:**
> Engage the discussion with Mike Rosulek and Fernando Virdia to initiate the project.

3.4. **Topics for the Crypto 2025 Strategic Meeting.** The Vice President is compiling topics for discussion at the *Crypto 2025 Strategic Meeting*. The following items are currently listed:

- Minimum criteria for selecting Program Chairs,
- Selection of the new Co-Editor-in-Chief for the journal *IACR Communications in Cryptology*,
- Discussion on conference and publication models,
- IT staffing considerations,
- Potential hosting of *Crypto* at other locations in the Americas.

Regarding the last topic, Schwabe notes that we have not yet contacted UCSB about their willingness to host *Crypto* every second year. Francisco proposes reaching out before the Strategic Meeting.

3.5. **IACR Election Committee update.** The *2025 Election Committee* will consist of: Rodríguez-Henríquez (chair), Yung, and Fiore. Naya-Plasencia will serve as an advisor. The Secretary reminds the Board that this year's election will be paired with a vote on amending the Bylaws.

4. CLOSING MATTERS

The President closes the meeting officially at 15:10 UTC.