MINUTES IACR BOARD MEETING *VIRTUAL-07 2025*

9 JULY 2025

1. Opening Matters

1.1. **Welcome, roll of attendees, identification of proxies.** At 14:05 UTC the 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: Halevi holds Bishop's proxy (when absent), LaMacchia holds Yang's proxy (when absent), Naya-Plasencia holds Rijmen's proxy, Naya-Plasencia holds Guo's proxy, Naya-Plasencia holds Wesolowski's proxy, Schwabe holds Preneel's proxy. As the Secretary is absent, Naya-Plasencia will be keeping notes of the meeting.

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); Shai Halevi (Director 2023-2025); Anna Lysyanskaya (Director 2025-2027); María Naya-Plasencia (Director 2024-2026); 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). Tal Rabin (Code-of-conduct Liaison); Andreas HÃ¼lsing (guest);

Absentees (Elected). Benjamin Wesolowski (Secretary 2023-2025); Jian Guo (Director 2025-2027); Bart Preneel (Director 2023-2025, Program Chair Contact);

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). Masayuki Abe (*Asiacrypt* Steering Committee); Gregor Leander (*FSE* Steering Committee); Tal Malkin (*TCC* Steering Committee); Kevin McCurley (Database Administrator); Hilarie Orman (Archivist); Yu Yu (Webmaster);

2. Membership survey about publication and conference issues

Bishop recalls that a working group has been drafting a survey for the Membership about publication and conference issues. She reports that by the end of the week, the draft will be sent to the wider Board for feedback.

3. RWC 2027 and 2028 Proposals

The RWC Steering Committee has submitted proposals for approval regarding *RWC 2027* and *RWC 2028*. LaMacchia recalls that RWC rotates between Asia, America, and Europe.

- *RWC 2027* is proposed to be held April 5-7, 2027, in Seattle, WA, USA, at Amazon's Meeting Center in downtown Seattle. Fixed costs are extremely low since the conference facility is being donated by the company. After a brief discussion, the President calls for a vote.

  Decision 1 (unanimous). *The Board approves the proposal to host RWC 2027 in Seattle.*

- *RWC 2028* is proposed to be held March 29-31, 2028, in Bochum, Germany, at the Jahrhunderthalle. Details on both proposals were sent by email to the Board ahead of the meeting. Bochum is centrally located in Europe and easily accessible. After a brief discussion, the President calls for a vote.

  Decision 2 (unanimous). *The Board approves the proposal to host RWC 2028 in Bochum.*

4. Discussion on Minimum Criteria for IACR Program Chair Selection

Halevi introduces the next topic: establishing minimum criteria for selecting program chairs (PCs) for IACR conferences, particularly focusing on publication records in relevant venues. This has been discussed several times over the years.

At the Strategic Meeting of *Eurocrypt 2024*, the Board decided not to establish formal requirements and instead continue selecting candidates through careful case-by-case considerations.

Halevi argues that some formal requirements would be beneficial. He collected statistics on publications by recent program chairs for IACR conferences (Asiacrypt, Crypto, Eurocrypt) compared to security conferences (as an example of a near-peer group). The data was used for statistical analysis in order to possibly improve future decisions. For each PC of Asiacrypt/Crypto/Eurocrypt of recent years, the number of publications within the same trio of venues was collected, and the same process was repeated for the trio CCS/Usenix/IEEE S&P. Halevi observed a notable discrepancy. He proposes voting to establish minimum criteria for IACR PC selection.

Yang asks for clarification on the problem being addressed: have there been issues with past selections that these criteria would prevent? He notes that PCs have generally performed well, and the rare problems were unrelated to their publication records. Halevi clarifies that this is not a functional issue but one of reputability and fairness. He mentions receiving feedback from individuals unhappy about the selection of some PCs with too few publications in IACR venues.

A lengthy discussion follows, weighing arguments for and against establishing formal criteria. The following arguments in favor of a minimum criteria are discussed:

- *Quality leadership indicator.* Publication records are an indicator for quality leadership. They reflect active engagement in the community, and familiarity with conference standards and practices.
- *Fair recognition.* Serving as a PC is an honor, and it is fair to reward more prolific researchers within the IACR community. A minimum criteria could mitigate perceived unfairness in selections.

The following arguments against a minimum criteria are discussed:

- *Uneven publication standards and underrepresented communities.* Strict publication requirements may exclude industry professionals and researchers from subfields with slower publication rate. Similarly, a criteria counting only publications in Asiacrypt, Crypto, and Eurocrypt will disfavor researchers whose publications are spread across different communities (security, hardware, number theory...).
- *Flexibility for Exceptional Cases.* Rigid criteria could disqualify outstanding candidates who excel in other ways. A case-by-case approach preserves flexibility.

No consensus emerges, but potential compromises are discussed:

- Define reasonable minimum criteria, with a mechanism to allow for exceptions.
- Ensure transparency by requiring justification for exceptions, and subject them to a (super)majority approval vote.

The conversation also touched on broader representation concerns. LaMacchia reports that some members feel their sub-community is underrepresented in General Conferences. It is proposed to discuss the matter further at the upcoming *Crypto 2025* Strategic Meeting.

Vote on Minimum Criteria Motion. Halevi proposes to vote on the following motion: *The board will establish a minimum criteria for serving as a Program Chair of the IACR flagship conferences (Eurocrypt, Crypto, Asiacrypt), including a higher bar for appointing exceptional people who do not meet this criteria.* Rabin seconds the motion.

LaMacchia tables the motion, so the President calls for a vote on whether we are ready to consider the motion.

Decision 3. *The Board decides to table the motion, deferring final action to a future meeting.*

5. Closing Matters

The President closes the meeting officially at 16:08 UTC.