MINUTES IACR BOARD MEETING *VIRTUAL-04 2025*

2 APRIL 2025

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 20 full time attendees with the following proxies: Lysyanskaya holds Halevi's proxy, Wesolowski holds Naya-Plasencia's proxy (when absent), Yang holds Rodríguez-Henríquez' proxy, Fiore holds Baldimtsi's proxy (when absent), Preneel holds Rijmen's proxy. 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); Brian LaMacchia (Treasurer 2023-2025, *RWC* Steering Committee); Benjamin Wesolowski (Secretary 2023-2025); Jian Guo (Director 2025-2027); Anna Lysyanskaya (Director 2025-2027); María Naya-Plasencia (Director 2024-2026); Bart Preneel (Director 2023-2025, Program Chair Contact); Peter Schwabe (Director 2023-2025, *CHES* Steering Committee); Bo-Yin Yang (Director 2025-2027); Moti Yung (Director 2024-2026, *PKC* Steering Committee);

Attendees (Appointed). Foteini Baldimtsi (Communications Secretary 2023-2025); 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); Joppe Bos (guest) Gregor Leander (*FSE* Steering Committee); Kevin McCurley (Database Administrator); Tal Rabin (Code-of-conduct Liaison);

Absentees (Elected). Shai Halevi (Director 2023-2025); Francisco Rodríguez-Henríquez (Director 2024-2026, *Crypto 2025* General Chair (2024-2025));

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

Absentees (Representatives and Others). Tal Malkin (*TCC* Steering Committee); Hilarie Orman (Archivist); Yu Yu (Webmaster);

2. UPDATE ON CONFERENCES

Fiore reports on the upcoming *Eurocrypt 2025*: everything is on track. Abdalla reports that the website of *Crypto 2025* has been changed to allow for remote presentations. LaMacchia suggests that we should discuss a uniform policy across our events for online presentations and attendance. It is a potential topic for the upcoming Strategic Meeting at *Eurocrypt 2025*.

3. TOPICS

3.1. **FSE 2026 proposal in Singapore.** A proposal to host *FSE 2026* in Singapore has been submitted to the Board for approval. The proposal has been shared with the Board ahead of the meeting. After a brief discussion, the President calls for a vote.

Decision 1 (unanimous)**.** *The Board approves the proposal to host FSE 2026 in Singapore.*

3.2. **Policy for conference presentation slides and videos.** McCurley summarizes the issue. We do not have a uniform, clear policy for conference submissions with respect to conference presentations, slides, live-streaming, and video recordings. For each conference, the General Chairs and Program Chairs will collaborate to write a call for papers with a policy that can vary slightly from year to year. There is also a general IACR-level policy, and another policy presented to the submitters when they submit on HotCRP. We should uniformize our policies and present to submitters a clear summary of what they are agreeing to when they submit.

One of the challenges is that each venue has a different way to deal with live-streaming and video recordings. We need to decide what the priorities are. Preneel notes that live-streaming is nice to have (maybe not a requirement), but video recordings are very valuable. Abdalla adds that we need a clear policy when authors do not wish to be recorded (for instance, because they do not wish their voice or face to appear online). One solution is to let these authors provide their own video recording (where they are free, for instance, not to use their own voice).

McCurley concludes: once we agree on a policy, it is important for it to be presented clearly to the authors at the time of submission.

Action Point **1:**
Draft a new policy for conference submissions regarding slides, live-streaming, and video recordings.

3.3. **Selection of Program Chairs for Crypto 2027.** The President recalls that we need to select the two Program Chairs for *Crypto 2027*. 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 2. *Stefano Tessaro is appointed Crypto 2027 Program Chair. [Tessaro has since accepted.]*

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

Decision 3. *Patrick Schaumont is appointed Crypto 2027 Program Chair. [Schaumont has since accepted.]*

3.4. **Discussion on long submissions.** Naya-Plasencia introduces the next item on the agenda. Some members have reached out to bring the attention of the Board to an ongoing discussion within the *Crypto 2025* program committee. The discussion concerns long submissions: how to handle submissions that are too lengthy to review within the limited time frame? Despite the page limit, submissions often include supplementary material. This supplementary material can be quite extensive and may contain essential information (such as a proof of the main claim). With such papers, reviewers find themselves unable to verify the correctness of the claims.

Yung questions the requirement for “correctness”: some very interesting papers rely on heuristics or models that do not accurately represent the real world (like random oracles). Wesolowski clarifies: the issue is about verifying whether the evidence presented in supplementary material is as solid as the paper suggests. If the main result is presented as a theorem, one expects it to be supported by a (correct) mathematical proof.

Long papers thus present a challenge. On one hand, the conference’s reviewing process does not allow reviewers to assess their correctness in a satisfactory manner. Furthermore, most accepted papers will not face any further peer review (it would be interesting to have statistics on “journal versions”). On the other hand, our conferences are the main publication venue of the field. Refusing results with long proofs denies them exposure and recognition.

Regarding *Crypto 2025*, the Board is not in a position to litigate: the Program Co-Chairs are entrusted with such decisions. However, for the long term, this matter ties in with our ongoing discussions on the publication model: a change of model could be an opportunity to improve the reviewing conditions and resolve the aforementioned issues.

3.5. **Policy on the use of generative AI in papers.** This discussion is postponed to the *Eurocrypt 2025 strategic meeting*, in May.

4. Closing Matters

The President closes the meeting officially at 16:05 UTC.