MINUTES IACR BOARD MEETING *VIRTUAL-10 2025*

9 OCTOBER 2025

1. Opening Matters

1.1. **Welcome, roll of attendees, identification of proxies.** At 14:03 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: Yang holds LaMacchia's proxy (when absent), Yung holds Lysyanskaya's proxy, Preneel holds Naya-Plasencia's proxy, LaMacchia holds Schwabe's proxy, Wesolowski holds Poettering'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); Bart Preneel (Director 2023-2025, Program Chair Contact); Francisco Rodríguez-Henríquez (Director 2024-2026, *Crypto 2025* General Chair (2024-2025)); Bo-Yin Yang (Director 2025-2027); Moti Yung (Director 2024-2026, *PKC* Steering Committee);

Attendees (Appointed). Foteini Baldimtsi (Communications Secretary 2023-2025); Edoardo Persichetti (*Eurocrypt 2026* General Chair (2025-2026)); Mayank Varia (*Crypto 2026* General Chair (2025-2026));

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

Absentees (Elected). Anna Lysyanskaya (Director 2025-2027); María Naya-Plasencia (Director 2024-2026); Peter Schwabe (Director 2023-2025, *CHES* Steering Committee);

Absentees (Appointed). Dario Fiore (Eurocrypt 2025 General Chair (2024-2025)); Joseph Liu (Asiacrypt 2025 General Chair (2024-2025)); Bertram Poettering (Membership Secretary 2023-2025); Vincent Rijmen (Journal of Cryptology Editor-in-Chief 2024-2026);

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

1.2. **Approving minutes from previous meetings.** The President calls for a vote to approve the minutes of the meetings *Virtual-09 2025*.

Decision 1 (unanimous)**.** *The Board approves the Minutes of the IACR Board Meetings Virtual-09 2025.*

2. Update on the 2025 IACR Election

Rodríguez-Henríquez provides a brief update on the organization of the 2025 IACR Election. Nominations have been received for all positions, and preparations are proceeding as planned. The Secretary invites comments regarding the text presenting the Bylaws amendment to the members.

3. Update on Conferences

Yang reports on *Asiacrypt 2025*. The program is being organized, with 144 accepted papers and three tracks. LaMacchia notes uncertainty regarding audiovisual setup (recording/online attendance). He suggests the Board consider enforcing minimum standards on these matters in the future.

Leander reports on *FSE*. The FSE steering committee is drafting formal Rules of Operation. Leander asks if Board approval is required; the President clarifies that while no formal approval is needed, the Board should review them to ensure alignment with IACR Bylaws.

4. TOPICS

4.1. **IACR 2027 Distinguished Lecture.** The board needs to select the person to deliver the IACR 2027 Distinguished Lecture (at *Asiacrypt 2027*). Three names have been submitted. Each candidate is presented in a few words by the person who nominated them. The President calls for a vote.

Decision 2. *The Board selects a nominee to deliver the IACR 2027 Distinguished Lecture at Asiacrypt 2027. A runner-up is also chosen in case the first nominee declines.*

4.2. **Test-of-Time committee selection.** The Board needs to appoint a new member for the Test-of-Time Award committee to replace Jean-Sébastion Coron. The next chair of the committee is Anne Canteaut. Two names have been proposed. Each candidate is presented in a few words by the person who nominated them. The President calls for a vote.

Decision 3. *A candidate is selected to join the Test of Time Award committee. [The person has since declined, and another candidate will be nominated during the next Board Meeting.]*

4.3. **Discussion on generative AI.** The IACR Board discusses the implications of AI tools (in particular large language models, LLMs), on cryptology research. McCurley briefly presents two main topics: crawling restrictions for the *Cryptology ePrint Archive* (ePrint) and policies regarding AI-generated content (for both authors and reviewers).

Policies on AI-Generated Content. AI-generated submissions are becoming an issue in ePrint: in the latest round, half of the submissions were rejected due to being AI-produced. These submissions are increasingly difficult for editors to distinguish at a glance, making the issue more time-consuming for the editors. A formal policy on AI-generated content is needed. The Board discusses the following points:

- *Transparency.* Authors should explicitly disclose any use of AI tools in their submissions, at least when such tools are used for substantive content (as opposed to minor stylistic or grammatical adjustments).
- *Author responsibility.* Authors remain fully accountable for their submissions, including any errors they contain. Human authors must verify that they understand and endorse their entire submission — including AI-generated sections.
- *Existing policies on authorship.* Several editors and archive servers already enforce rules prohibiting AI from being listed as an author, insisting on human responsibility.
- *Endorsement systems.* A structured endorsement system (similar to ArXiv's) could help reduce the number of AI-generated submissions.
- *Dedicated AI channel.* An alternative approach would be to create a separate channel or section specifically for AI-generated papers. It could provide a space for experimentation and playful exploration without overwhelming the main archive.

The following points are made about the use of generative AI by reviewers:

- *Assistive role.* LLMs can generate summaries, assist with grammar, and refine draft reviews — helping reviewers work more efficiently.
- *Human accountability.* AI tools should not replace critical reading or decision-making. The final review must remain with human experts, who are responsible for ensuring depth of analysis, fairness, and adherence to ethical standards.
- *Confidentiality risks.* Caution is required when using third-party AI tools on confidential submissions. Reviewers should avoid sharing sensitive content with external platforms.

The Board concludes that the policy on AI-generated content should insist on human accountability. Detecting the use of AI is increasingly difficult, let alone *proving* it. It is easier to enforce rules on the quality of submissions that on their origin.

Crawling Restrictions. A member raised concerns via email about crawlers being blocked from accessing ePrint papers. This restriction makes it inconvenient to use AI tools (e.g., summarizing papers through links) and diminishes the quality of models by denying them training on the field's authoritative source.

The following points are discussed.

- **Legitimate use.** There are numerous legitimate applications, such as summarizing papers. While users can bypass restrictions for single papers by uploading PDFs directly to AI tools instead of using links, this approach is impractical for broader tasks like analyzing recent activity in a subfield or searching references.
- **Community trust.** The use of ePrint's resources for training AI models raises concerns among the Board. Authors may not have anticipated their work being repurposed for AI training without explicit consent,

mirroring issues faced by the creative industry. While ePrint promotes openness, it is argued that its primary role is to serve cryptologists, not to facilitate corporate AI development.

- **Reinforcing the problem of AI-submissions.** Models trained on ePrint data could accelerate the problem of AI-generated submissions by enabling content generation that is even harder to distinguish (even if only stylistically). It is acknowledged, however, that this may be an unavoidable challenge in the long term.
- **Enforcement challenges.** Distinguishing between crawlers used for research and those employed for training AI models is difficult. While crawlers declare their intent, there is no way to verify how the data will ultimately be utilized. Contractual agreements with companies could allow controlled access, but the Board does not favour this approach.

The President invites opinions on whether ePrint should open access to crawlers. Some members express uncertainty about the implications of such a decision. Most Board members are currently uncomfortable with opening access, as it would be a permanent move. The Board agrees to form a committee (comprising Abdalla, McCurley, and Varia) to further explore this issue and address it formally. It is also noted that these challenges will likely evolve rapidly as AI technology advances.

5. Closing Matters

The President closes the meeting officially at 16:01 UTC.