MINUTES IACR STRATEGIC MEETING AT *CRYPTO 2025*

17 AUGUST 2025

1. Opening Matters

1.1. **Welcome, roll of attendees, identification of proxies.** At 9:27 CEST the Vice President opens the meeting. The President will arrive later during the meeting. The Secretary is confirming attendees and establishing who is holding proxies.

There are 20 full time attendees with the following proxies: LaMacchia holds Schwabe's proxy (when absent), Abdalla holds Poettering's proxy, Bishop holds Varia'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); 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 (online, Director 2023-2025, *CHES* Steering Committee); Bo-Yin Yang (Director 2025-2027); Moti Yung (Director 2024-2026, *PKC* Steering Committee);

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

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

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

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);

The Vice President rapidly goes through the items on the agenda, and the Board decides on an order.

2. General discussion on the situation of the association

2.1. **Financial update.** LaMacchia presents a report to the Board on the financial situation of the IACR. The largest expenses are related to conference organization, followed by student stipends. New expenses include insurance and accounting services. After a detailed presentation, LaMacchia opens the floor for questions. McCurley observes that, compared to other scientific associations, the IACR appears to operate at a relatively low cost.

2.2. **Involving younger members.** Halevi remarks that the average age of Board members seems to have increased over the years. He encourages the Board to reflect on this trend: do younger members volunteer less, or has the scale of the organization become more intimidating?

Naya-Plasencia points out that young candidates often run for the Board but tend to lose elections to more senior, well-known members — frequently incumbent Board members seeking re-election. Bishop adds that joining the Board can be a daunting step for newcomers. She suggests considering a pipeline to engage volunteers through less demanding roles first.

3. Selection of the co-Editor-in-Chief of *Communications in Cryptology*

The Vice President introduces the next agenda item: the selection of a new co-Editor-in-Chief for *Communications in Cryptology*, to succeed Andreas Hülsing. Five candidates have been nominated. The President arrives and assumes leadership for the remainder of the meeting. He calls for a vote.

Decision 1. *Elisabeth Oswald is appointed co-Editor-in-Chief of* Communications in Cryptology. *[Oswald has since accepted the appointment.]*

4. Survey on publication and conference model

The survey on publication and conference model has been launched. The Board agrees to wait for the survey results before proceeding with further discussion.

5. Evaluating and publishing artifacts

The President introduces the next agenda item: the evaluation and publication of artifacts in all our publication venues. The Board agrees on the importance of investing in artifact storage as a key component of scientific openness and reproducibility. However, managing artifacts associated to research submissions raises financial, logistical, and policy issues.

Two significant datasets (one 90GB and another 600GB) are cited as examples, raising concerns about long-term storage costs. LaMacchia cautions that establishing a formal policy could create financial liabilities for the association. The submission of very large datasets could remain at the discretion of each Program Committee.

Abdalla suggests implementing a cap on guaranteed hosting capacity for all our venues, and larger artifacts could be handled on a case-by-case basis. Halevi proposes setting this threshold as a dollar-value limit per artifact, though the cumulative cost across annual conferences remains a concern.

The next point concerns the lack of a uniform policy across IACR events: should all conferences allow for the submission of artifacts? The Secretary notes the absence of an artifact call at Crypto this year. Each conference (or, at least, our General Conferences) could be required to have a committee for the evaluation of artifacts. Alternatively, artifact evaluation could be centralized with a shared platform and committee for all IACR venues.

The Board proposes to appoint an IACR Artifacts Committee, whose first task would be to develop guidelines for the evaluation and publication of artifacts. This committee will address budgetary considerations and ethical issues (such as those related to attack code). Once these guidelines are established, the role of the committee would be to provide continued support and advice on the matter.

Decision 2. *The Board agrees to form an IACR Artifacts Committee to develop guidelines for artifact evaluation and publication.*

The Board agrees that Schwabe (absent today) would be a good candidate to lead the effort. The Secretary will extend him an invitation. The Board would like the committee to draft guidelines before March 2026, ahead of the Eurocrypt 2026 strategic meeting.

6. New position of IT Manager

The Secretary introduces the next agenda item: the latest version of the Bylaws amendment, which includes a new article establishing the role of IT Manager, has been shared by email. He solicits the Board's feedback on this article. The article proposes that the IT Manager serves as an appointed Board member. The Board approves the proposal. The Secretary invites further comments on the article via email and reminds the Board that this Bylaws amendment will be submitted to the Membership for approval later this year.

Bishop suggests announcing at Crypto that the association will seek candidates for this new position. She encourages the Board to begin considering potential candidates.

The President calls for a break at 12:10. The Board reconvenes at 12:52.

7. Hosting Crypto at UCSB or other venues

The President introduces the next agenda item: exploring the possibility of hosting Crypto at venues other than the traditional UC Santa Barbara. Bishop and LaMacchia have initiated discussions with UCSB about potentially hosting Crypto there every second year, instead of every year.

Some members face challenges attending events in the United States, and rotating the conference location within the Americas could enable broader participation. Retaining UCSB as a venue every second year would help preserve a valued community tradition.

Additional factors motivating this change include rising costs at UCSB and the decline in attendance this year — dropping below 400 for the first time since 2015. This decrease is likely linked to increased difficulties in entering the country, and budget cuts affecting travel within the United States.

The Board agrees to begin experimenting by issuing a call for proposals to host Crypto elsewhere in 2027 or 2028, open to venues across the Americas. Lysyanskaya volunteers to draft the call.

> Action Point **1: Lysyanskaya**
> Draft and advertise a call for proposals to host Crypto 2027 or 2028.

To streamline the process, the Board decides to request expressions of interest by the end of September, with full proposals due by the end of the year. Lysyanskaya proposes to announce the call during the Crypto rump session.

7.1. **Student travel support.** The decline in attendance at *Crypto 2025* prompts a discussion on student travel support. While waiving registration fees for student speakers is helpful, it is often insufficient when students lack funds. LaMacchia raises the question of whether the association should increase its role in funding student travel. This could be achieved through a more robust sponsorship strategy and by allocating a portion of investment revenues to support students.

8. Requirements for Program Chairs

Halevi introduces the next agenda item: establishing minimum criteria for selecting Program Chairs (PCs) for IACR conferences. He presents data indicating that, compared to neighboring communities, the publication profiles of IACR PCs count a noticeable number of outliers. Specifically, several PCs of the General Conferences have had relatively few publications in these same conferences (and instead, more publications in other specialized venues).

The Board broadly agrees that some minimum requirements (such as a history of publishing in IACR or related venues) would be beneficial. However, concerns are raised about potentially excluding researchers from subfields underrepresented in General Conferences. Selection criteria should balance publications in these conferences with broader contributions to the research community, allowing for exceptions when justified. As IACR events grow, the organizational skills of Program Chairs become increasingly important, and formal criteria focused solely on publication records may not capture these qualities.

Representation and balance among areas. A key concern is the perceived imbalance in the representation of subfields at our General Conferences. In particular, CHES and RWC are noted as underrepresented. The Board debates potential causes, including submission volume per area, acceptance rates, and self-selection biases. There is discussion about whether General Conferences should seek to address these imbalances.

Abdalla highlights the situation of RWC: articles presented at this Symposium have often been published in non-IACR venues, typically in the security community. Rodríguez-Henríquez insists that all researchers in cryptography should feel welcome to submit their work to our General Conferences.

Proposed Criteria and Process. The discussion focuses on three potential criteria for PC selection:

- Publication record: a minimum number of publications in IACR or related venues. It is suggested that any mandatory minimum threshold should be set low to avoid excluding candidates with atypical profiles. A threshold of five publications over the past five years is mentioned.
- Breadth of research: exposure to multiple subfields is highly valuable, given the scope of General Conferences. It is noted that having two Co-chairs helps ensure breadth.
- Organizational experience: prior experience in roles such as Area Chairs, or Program Chairs for smaller events. Bishop suggests that the role of Area Chair could serve as a pipeline for future Program Chairs.

Decision. The Board agrees to form a committee to draft specific criteria for PC selection. Halevi, Naya-Plasencia, Schwabe, and Preneel volunteer to serve on this committee.

> Action Point **2:**
> The committee will prepare a proposal establishing minimum criteria for the selection of Program Chairs.

9. Various topics

9.1. **Restaffing committees.** The President introduces the next agenda item: several committees are currently understaffed. The Ethics Committee requires two new members, and the Schools Committee needs one new member. The President invites the Board to identify volunteers, who do not need to be Board members.

9.2. **Moving to in-house publishing.** Depending on the results of the ongoing survey on publication and conferences, the Board may consider transitioning conference proceedings from Springer to in-house publishing. McCurley has investigated the feasibility of this change and confirms that it is technically viable.

9.3. **Authorship responsibility.** McCurley raises concerns related to authorship responsibility. The 2025 Usenix conference[1] reported serious issues, including 14 authors listed on at least 15 submissions each, and one author listed on 39 submissions. The report noted that "at such volume, it becomes difficult not to question the nature and depth of the contributions attributed to these individuals." While such cases have not been observed within the IACR community, the Board may wish to monitor the situation.

McCurley also recalls that, during the *Eurocrypt Strategic Meeting*, the Board discussed challenges posed by generative AI, particularly its use in writing articles or reviews. He offers to draft a policy governing the use of AI in submissions.

10. Closing Matters

The President closes the meeting officially at 17:01 UTC.

[1] https://www.usenix.org/sites/default/files/sec25_message.pdf