MINUTES IACR STRATEGIC MEETING AT *EUROCRYPT 2026*

10 MAY 2026

1. Opening Matters

1.1. **Welcome, roll of attendees, identification of proxies.** At 09:50 CEST the President opens the meeting and briefly goes around for an introductory round, confirming attendees and establishing who is holding proxies.

There are 22 full time attendees with the following proxies: Lysyanskaya holds Varia's proxy (when absent), Lysyanskaya holds Halevi's proxy (when absent), Naya-Plasencia holds Rijmen's proxy.

1.1.1. *Roll of Attendees.*

Attendees (Elected). Allison Bishop (President 2026-2028); François-Xavier Standaert, (Vice President 2026-2028); Brian LaMacchia (Treasurer 2026-2028, *RWC* Steering Committee); Benjamin Wesolowski (Secretary 2026-2028); Jian Guo (online, Director 2025-2027); Shai Halevi (online, Director 2026-2028); Anna Lysyanskaya (Director 2025-2027); María Naya-Plasencia (Director 2024-2026); Bart Preneel (Director 2026-2028, Program Chair Contact); Francisco Rodríguez-Henríquez (online, Director 2024-2026); Bo-Yin Yang (Director 2025-2027, *Asiacrypt* Steering Committee); Moti Yung (Director 2024-2026, *PKC* Steering Committee);

Attendees (Appointed). Andreas Hülsing (online, *Eurocrypt 2027* General Chair (2026-2027)); Tetsu Iwata (online, Asiacrypt 2027 General Chair (2026-2027)); Edoardo Persichetti (*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 (online, Database Administrator);

Absentees (Elected). Peter Schwabe (Director 2026-2028, *CHES* Steering Committee);

Absentees (Appointed). Man Ho Allen Au (Asiacrypt 2026 General Chair (2025-2026)); Foteini Baldimtsi (Communications Secretary 2023-2026); Joppe W. Bos (IACR Communications in Cryptology Editor-in-Chief); Chitchanok Chuengsatiansup (Membership Secretary (2026-2028)); Vincent Rijmen (Journal of Cryptology Editor-in-Chief 2024-2026);

Absentees (Representatives and Others). Tal Malkin (*TCC* Steering Committee); Kay McKelly (Web & software developer); Hilarie Orman (Archivist); Tal Rabin (Code-of-conduct Liaison); Yu Yu (Webmaster);

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

2. Schools Committee

Francisco Rodríguez-Henríquez, as chair of the Schools Committee, presents two summer school proposals:

- The Africacrypt Summer School in Hammamet (July 6–7), requesting €14,520 (approximately $17,000). They expect an attendance of 70 people.
- A Summer School in Hanoi (August 22–28), requesting $10,000.

LaMacchia notes that while the Africacrypt request exceeds typical funding levels, the event is an important opportunity to support cryptography in Africa. If IACR does not provide full funding, it may be difficult for the organizers to secure the remaining amount.

The President calls for a vote.

Decision 1 (unanimous)**.** *The Board approves sponsoring both schools for their full requested amounts.*

3. IT MANAGER

The new Board position of *IT Manager* was recently approved by the IACR Membership. Since then, the Board has been seeking candidates. Tancrede Lepoint has volunteered for the position. McCurley expresses his support for Lepoint, and the President calls for a vote.

Decision 2 (unanimous)**.** *The Board appoints Tancrede Lepoint as IT Manager for a three-year term.*

The President calls for a 20-minute coffee break; the Board reconvenes afterward.

4. CRYPTO 2027

The Board considers a proposal to host *Crypto 2027* in Bogotá, Colombia, with Valerie Gauthier-Umaña as General Chair. The campus offers four large auditoriums, and cheap accommodation. The estimated registration fees are comparable to UCSB, or slightly cheaper.

The Board appreciates the quality of the proposal. Some concern about the timeline is expressed: 2027 is getting close, and we may not want to rush such a significant move. Negociations with UCSB for 2027 have progressed, and moving away in 2028 may be more favorable. Bishop proposes discussing with Gauthier-Umaña about the possibility to host *Crypto 2028* in Bogotá.

The Board decides to delay the selection of the *Crypto 2027* General Chair pending further discussion and clarification from the proposers regarding their flexibility on timing.

> Action Point **1: Bishop**
> Contact the Bogotá proposers to discuss the possibility of considering their bid for 2028 instead of 2027.

Leandre suggests we take the opportunity of the upcoming Membership Meeting to poll the community about hosting *Crypto* in Bogotá.

5. PUBLICATION MODEL

The working group on the publication model has finalized its draft proposal and distributed it to the Board. Before opening the discussion, Bishop informs the Board that Springer is open to renegotiating our contract to accommodate the model change. Springer would offer certain advantages if we commit to staying with them a few more years. However, the Board is reminded that the 2025 community survey clearly indicates a preference for open access publishing.

Regardless of whether we extend our contract with Springer, there is concern about the model change disrupting the indexing and ranking of our publications. The process of journal and conference ranking is not transparent. The normal practice seems to be that conference rankings are preserved, as demonstrated by PETS/PoPETS, FSE/ToSC and CHES/TCHES; this will require ensuring clear continuity for each conference in terms of branding, metadata, etc. However, a new hybrid journal will not be ranked *as a journal* for its first few years of existence.

The Board discusses various details of the proposal:

- Balancing the number of papers among conferences and among areas (and how this affects the local organization of the conferences).
- How the proposal addresses the increasing reviewing load.
- Which decisions are left to Editors-in-Chief and which require Board approval (like the selection of Area Chairs or the presentation format).
- The selection of an initial list of areas. The proposal suggests starting from the areas of *Communications in Cryptology* (CiC). Wesolowski suggests asking the CiC editors if they think their current areas are balanced.
- How the proposal affects the geographic division of the community. The attendance of each conference is already biased by geographic proximity. Will the proposal increase this bias? This would be consistent with the increasing pressure to reduce travel by plane.

Naya-Plasencia invites the Board to send any additional feedback as soon as possible. The Board agrees on the following approach:

(1) The working group will meet soon to incorporate the latest comments.
(2) The draft proposal will be made public in June and presented as a compromise that the Board fully supports.
(3) The community will be given the opportunity to share feedback, either by email or on a discussion platform.
(4) The working group on the publication model will address any concerns raised.
(5) The Board will then vote on a final version, to be approved by the Membership via a referendum during the summer.

6. Conference Experience

A second working group has focused on the conference experience. The survey results on this topic were not as clear-cut as those for publication-related matters. There is a general understanding that it will be difficult to maintain both the current acceptance rate and 20-minute talks for all papers, thus requiring a change.

The working group has considered how much freedom to give Program Chairs and General Chairs regarding the conference format. Flexibility is valuable for adapting to local organizational constraints, accommodating variability in the number of submissions, or addressing unexpected events affecting travel.

However, setting guardrails for conference format will help ensure continuity. The working group considered two approaches:

- Developing a standard list of options available to the Chairs (e.g., talks of a certain length, posters);
- Disallowing certain options (such as extremely short talks).

The working group has also discussed ways to better synchronize related talks. Talks in the same session often share background requirements, in which case joint background material could be distributed in advance. This could reduce the impact of shortening the talk slots. However, it may be difficult for authors of different submissions to synchronize and produce such background material.

The Board takes a break at 12:41 and reconvenes at 14:10.

7. FSE 2027 Proposal

The *FSE 2027* proposal for Maastricht, Netherlands is presented, with Bart Mennink as General Chair. The university venue offers low costs, and a backup plan is proposed if the campus is unavailable. The conference would run for four days, with a spring school preceding it.

The President calls for a vote.

Decision 3 (unanimous)**.** *The Board approves the proposal to host FSE 2027 in Maastricht, Netherlands.*

The Board enters an executive session.

The President calls for a break at 15:17; the Board reconvenes at 15:49.

8. Conference Experience (Continued)

(Note: part of the following discussion has been moved to Section 5 for clarity)

The President reopens the discussion on the conference experience by raising the question of in-person presentations. Various Program and General Chairs have taken different positions regarding this matter. For example:

- The *Eurocrypt 2026* call for papers strictly requires accepted papers to be presented in person at the conference by one of the authors.

- The *Crypto 2026* call for papers explicitly allows accepted papers to be presented remotely if the authors so choose.
- *PKC 2026* allowed remote presentations but charged full registration fees for remote presenters.

The IACR should have a uniform policy on this matter, at least for the three General conferences.

Naya-Plasencia notes that, in the working group on the publication model, a majority believes presentation should not be mandatory. Indeed, our General conferences are the most prestigious publication venues in cryptology, and they should be open to all researchers in the field. By imposing in-person attendance, some researchers are denied publishing in these venues (because of pregnancy, disabilities, limited budgets, etc).

In the draft proposal for a new publication model, authors must choose a conference when they submit an article; if they do not expect to be able to travel, they may simply warn the Editor-in-Chief.

Preneel supports mandating that video presentations be available online for all accepted papers (either recorded during the event or pre-recorded). The survey results indicated strong support for this.

9. Closing Matters

The President closes the meeting at 16:43 CEST.