MINUTES IACR STRATEGIC MEETING AT *EUROCRYPT 2025*

4 MAY 2025

1. Opening Matters

1.1. **Welcome, roll of attendees, identification of proxies.** At 10:24 CEST 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: Bishop holds Halevi's proxy, Bishop holds Varia's proxy (when absent), Yang holds Guo'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 (online, Director 2025-2027); Anna Lysyanskaya (online, 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 (Director 2023-2025, *CHES* Steering Committee); Bo-Yin Yang (Director 2025-2027); Moti Yung (online, 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 (online, *Crypto 2026* General Chair (2025-2026)); Bertram Poettering (Membership Secretary 2023-2025);

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

Absentees (Elected). Shai Halevi (Director 2023-2025);

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); Tal Malkin (*TCC* Steering Committee); 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. Strategic goals for the IACR

The President introduces the first topic: rethinking critical aspects of our organization, particularly our publication and conference model, to address new challenges. To guide these discussions, we must clearly define the main goals for the IACR.

Our organization is experiencing significant growth, with rising numbers of submitted and accepted papers, as well as increasing attendance at General Conferences. Eurocrypt 2025 has set a new record with 123 accepted papers. This expansion poses challenges that require balancing multiple priorities:

- Gathering the community (across scientific sub-disciplines and geographic regions),
- Ensuring a pleasant and fruitful conference experience for attendees,
- Upholding high scientific standards,
- Preserving a reasonable acceptance rate,
- Offering an efficient publication and dissemination platform,
- Maintaining reasonable costs across all operations,
- Reducing the environmental and social impact of travel.

Bishop proposes an ambitious goal: rapidly establishing a publication and conference model that can sustain the IACR for the next 10 to 15 years. The discussion explores potential changes, each with its own advantages and drawbacks:

(1) *Decoupling publication from presentation.* We could reduce the correlation between publication and presentation slots. In a hybrid journal-conference model, submissions go to a journal, which handles peer review and publication. The conference program would be based on the accepted publications (with more flexibility than the current format) to optimise for the best conference experience.

(2) *Advantages of a journal-first approach.* A journal offers more flexible submission and reviewing deadlines. Longer papers benefit from extended review times, improving quality. A single journal serving as a unified platform for *Asiacrypt*, *Crypto* and *Eurocrypt* could provide a clearer, unified quality stamp (e.g., synonymous to being the top 20% of the field). Also, flexible distribution to conferences could ease travel concerns.

(3) *Disadvantages of a journal-first approach.* Moving to a journal conflicts with CS conference culture, where work is primarily evaluated via conferences (via A* ratings). Preneel notes that DORA (San Francisco Declaration on Research Assessment) discourages metric-based evaluation, but cultural inertia persists. Naya-Plasencia advises that our decisions shouldn't be based on disagreeable *status quo* practices.

(4) *Improving the conference experience.* The current three-track format is reaching its limits, with packed schedules degrading the experience. Shorter talks, longer days or more tracks (to accommodate the increasing number of submissions) would degrade it further. The Board discusses the different alternatives. A program centered on invited talks, panels, best-paper selections and community events might be more fruitful. Wesolowski notes that decoupling publication from presentation enables this: Program Chairs could craft a program optimized for best conference experience.

(5) *The importance of talks and representing each article.* The Board identifies the following three purposes for talks:
   - Disseminating research results,
   - Offering exposure and experience to the young researchers, and
   - Enabling travel (some employers cover travel only if their researcher gives a presentation).

   Alternatives to traditional talks could include posters, lightning sessions, or video recordings. Some priority could be given to young speakers for a traditional talk slot.

(6) *More room for affiliated and colocated events.* Schwabe observes that affiliated events are increasingly popular. Lightening the main program's schedule could accommodate more affiliated events. LaMacchia adds that having a robust affiliated program might also attract broader audiences (from neighboring domains, and from sub-communities that do not publish much, like the industry).

(7) *Increasing the number of events.* Rodríguez-Henríquez suggests increasing the number of conferences. It would help distribute the load, and reach more regions of the globe. This raises logistical challenges: an increased workload on volunteers, and treasury strain. LaMacchia notes that we are occasionally approached by conferences looking to integrate the IACR. A rare few would be good fits. However we first need to define our strategic goals.

There is broad agreement that decoupling publication from presentation is beneficial, though full decoupling may introduce new issues.

Community survey. There appears to be a need for a significant redesign, so the working group should draft a concrete proposal to share with the IACR community. Given the diversity of alternatives and opinions, Bishop proposes conducting a structured survey process. First, the working group will gather input from Board Members. Bishop will initiate this via email in the near future.

Action Point **1: Bishop**
Collect feedback from Board Members on the evolution of the IACR publication and conference model over the next decade.

This initial feedback will inform a broader survey for the entire community.

Action Point **2: Working group on the publication and conference model**
Design a community-wide survey about the publication and conference model.

The goal is to finalize this survey before the *Crypto 2025 Strategic Meeting* in August. Based on results, the working group will develop a concrete proposal which will be submitted for Board review and voted upon by IACR Membership.

Action Point **3: Working group on the publication and conference model**
Develop a formal proposal for the new publication and conference model based on survey responses.

3. Policies on the use of generative AI in scientific submissions

The following issue was first raised by the *Cryptology ePrint Archive* Editors but extends to all our publications: we need a policy on the use of generative AI in scientific submissions.

For reference, Preneel explains that his university's policy authorizes AI-tools for spell-checking and phrasing, while any other uses (e.g., code generation) must be properly documented. This policy is regularly updated. Abdalla reports that major associations (ACM, IEEE, etc.) accept AI-tool use but emphasize that the work remains entirely the responsibility of its (human) authors. Key examples include:

- ACM states that AI used to "generate new content" must be disclosed, and clarifies that spell-checking does not fall in that category.
- PETS further mandates disclosing both the model and prompt used.
- ArXiv prohibits listing AI-tools as authors or blaming them for inaccuracies.

Yang raises concerns about entire sections appearing to be AI-generated without acknowledgment. To what extent should AI-tool use be disclosed? Schwabe notes that detecting AI usage is increasingly difficult, yet a policy remains necessary (even if it is hard to enforce). Abdalla proposes to work on a draft, using the aforementioned examples as reference.

Action Point **4: Abdalla**
Draft a policy on the use of generative AI in scientific submissions.

Bishop notes that we also need a policy on the use of AI for reviewing. Wesolowski observes that submission confidentiality already prohibits online tools like ChatGPT, though the question of locally run models remains open.

Action Point **5:**
Discuss and draft a policy on the use of AI for reviewing.

The President calls for a break at 12:40; the Board reconvenes at 13:30.

4. Challenges of reviewing long papers for conferences

The next topic follows concerns raised by members of the *Crypto 2025* Program Committee. Some papers are too long to review thoroughly within tight deadlines, raising concerns about correctness verification. Opinions diverge on whether conference submissions should demand full verification or prioritize speed (with deeper analysis reserved for journals).

It is noted that a hybrid journal-conference model could mitigate this issue by offering more flexible reviewing timelines for long papers.

Abdalla notes that Program Chairs have broad discretion. The Board can set general guidelines, but editorial decisions ultimately rest with them.

Yung suggests letting Program Chairs apply their own judgment on this matter. The Board's influence lies in selecting the Program Chairs. Mayank highlights potential confusion for authors if expectations are unclear.

Preneel advocated for a single strict rule: publish only the part that has been reviewed (i.e., the portion fitting within page limits).

5. Initiatives for educational material on cryptography

Mike Rosulek and Fernando Virdia submitted a proposal to the Board regarding the dissemination and production of high-quality educational material in cryptography both in English and in underrepresented languages. Specifically, they propose:

- The creation of a library of open-access educational resources, and
- The publication of special issues of educational material (for instance, in the *IACR Communications in Cryptology*).

They request that IACR hosts the library to lend legitimacy and propose designing its web interface themselves. The Board appreciates these ideas. Schwabe notes that long-term maintenance will be required, and suggests reliance on a collaborative platform like GitLab. Abdalla proposes following up with Rosulek and Virdia directly.

On a related matter, Wesolowski proposes encouraging the production of Systematization-of-Knowledge (SoK) papers. These are valuable to the community and should be incentivized; publishing high-quality SoK at IACR's General Conferences would serve as a strong motivator. The Board agrees.

The *Program Chair* guidelines currently do not address the matter. Bishop observes that implementing such a change would be straightforward: simply adding SoK papers to the call-for-papers scope.

6. Challenges with travel and conference locations

Bishop introduces the next agenda item: ongoing or increasing issues are affecting attendees' ability and willingness to travel to conferences. These challenges include visa difficulties, climate change concerns, political tensions, and income/funding disparities. To mitigate these issues, the IACR could reduce travel requirements by making in-person attendance optional for authors.

Abdalla notes that remote events performed well during COVID-19, and some events still offer remote options. At *Eurocrypt 2025*, approximately 15 attendees are registered remotely — a scale that minimally impacts the budget. LaMacchia adds that if demand grows, a small fee could offset infrastructure costs for remote participants.

Currently, remote access is primarily offered to the audience. Speakers are only offered to present virtually in exceptional cases. Growing travel barriers have fueled sentiment against mandatory attendance for speakers, but remote talks at in-person events remain unpopular.

Yung emphasizes the value of in-person engagement, and is worried that the attendance will decrease if speakers are no longer required to travel. Persichetti responds that most authors still prefer presenting in person when given the choice.

Mayank notes that online tools offer benefits: for instance, they allow a live exchange for questions and clarifications without disrupting the talk.

Schwabe proposes separating short-term solutions (e.g., addressing visa issues) from long-term strategy, as the change of conference model will impact this discussion.

7. Organizational staffing

Bishop introduces the last agenda item. At the *Crypto 2024 Strategic meeting*, the Board agreed that professional services will be needed to handle tasks currently managed by McCurley.

McCurley explains these responsibilities fall into two profiles: Linux system administration, and web development. For maintenance alone, he estimates one full-time position suffices; Bishop suggests hiring two, as maintenance is only one aspect of the work. They will need to be available, and to create documentation and an easily maintainable infrastructure.

Candidates could be freelancers or employees, though Schwabe notes that some jurisdictions require full-time workers to be formal employees.

McCurley adds that a Board Member should oversee these roles. The Secretary proposes creating an appointed IT Manager position on the Board (responsible for hiring and managing IT staff, ensuring a continuity in the infrastructure, communicating decisions of the Board that need IT action...).

Action Point **6: Wesolowski**
Draft Bylaws amendment to formalize the IT Manager role on the Board of Directors.

Action Point **7: Everyone**
Identify candidates for IT Manager.

While it is primarily a management position, the ideal candidate would be familiar with Linux system administration and web development.

It is suggested that the IT staff is hired locally by the IT Manager to facilitate in-person collaboration.

Bishop urges prompt action, and McCurley volunteers to draft job descriptions for IT roles.

Action Point **8: McCurley**
Prepare job description(s) for IT staff hiring.

8. Closing Matters

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