MINUTES IACR STRATEGIC MEETING AT *CRYPTO 2024*

18 AUGUST 2024

1. Opening Matters

1.1. **Welcome, roll of attendees, identification of proxies.** The President opens the meeting and briefly goes around for an introductory round, confirming attendees and establishing who is holding proxies. There are 21 full time attendees. The Secretary is attending remotely, and Schwabe, attending in person, offers to take notes.

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 (online, Secretary 2023-2025); Anna Lysyanskaya (online, Director 2022-2024); Bart Preneel (Director 2023-2025, Program Chair Contact); Francisco Rodríguez-Henríquez (Director 2024-2026); Peter Schwabe (Director 2023-2025, *CHES* Steering Committee); Bo-Yin Yang (online, Director 2022-2024); Moti Yung (Director 2024-2026, *PKC* Steering Committee);

Attendees (Appointed). Tancrède Lepoint (*Crypto 2024* General Chair (2023-2024));

Attendees (Representatives and Others). Kevin McCurley (Database Administrator); Hilarie Orman (online, Archivist);

Absentees (Elected). Jian Guo (Director 2022-2024); Shai Halevi (Director 2023-2025); María Naya-Plasencia (Director 2024-2026);

Absentees (Appointed). Foteini Baldimtsi (Communications Secretary 2023-2025); Dario Fiore (Eurocrypt 2025 General Chair (2024-2025)); Julia Hesse (online, *Eurocrypt 2024* General Chair (2023-2024)); Joseph Liu (Asiacrypt 2025 General Chair (2024-2025)); Bertram Poettering (Membership Secretary 2023-2025); Vincent Rijmen (Journal of Cryptology Editor-in-Chief 2024-2026); Bimal Roy (*Asiacrypt 2024* General Chair 2023-2024);

Absentees (Representatives and Others). Gregor Leander (*FSE* Steering Committee); Tal Malkin (*TCC* Steering Committee); Mitsuru Matsui (*Asiacrypt* Steering Committee); 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. Treasury

LaMacchia opens the first item on the agenda with an overview of the services handled by the IACR Treasury. He then brings a few questions to the Board's attention.

- Who should be the secondary signer for IACR financial accounts? He proposes that Bishop be the secondary signer. Schwabe asks whether we should formalize the selection of a secondary signer, and whether they must be from the US. It might make things easier, but Preneel recalls that he used to have secondary signing rights despite being located in Europe.
- Should the IACR keep its French bank account for payments in Euro? The President will look into the matter more closely before making a decision.
- LaMacchia proposes to centralize all student travel stipends to the IACR Treasury. The Board agrees. LaMacchia asks whether the IACR should become an NSF grant-receiving organization and take over direct management of NSF travel grants. The Board will keep this possibility in mind for future consideration, once the new financial services are set up.
- LaMacchia is currently working on a proposal for the IACR to contract professional accounting-related services. Until now, the Treasurer has managed all accounting and bookkeeping tasks for the association. However, with the IACR's growth, this is no longer feasible without additional assistance. The Board approves this initiative. It will ease the transition to future Treasurers. LaMacchia will soon present a concrete proposal including a detailed list of services.

- The Treasurer proposes to increase the IACR membership fees to USD 80 (regular) and USD 40 (student). This increase is justified by the increased cost for financial services, IT, the new journal *IACR Communications in Cryptology*, and inflation over the last ten years. The Board agrees, and the proposal will be submitted to this week's Assembly.

Action Point **1: LaMacchia**
Draft a proposal for the IACR to contract professional accounting-related services.

3. IT STAFFING

McCurley presents the next item on the agenda. He presents a few slides listing various IT tasks he has been handling for the IACR, including large-scale software projects (HotCRP, CiC, ePrint, publish.iacr.org, etc.) and maintenance tasks (servers, updates, user accounts, etc.). Maintenance alone takes McCurley ten hours per week. We need to find a solution for other people to get involved or take over: either outsourcing or finding volunteers within the IACR. Building strong documentation should be a priority to ease future transitions. The Board agrees that hiring professional services will be needed. McCurley will write a job description.

Action Point **2: McCurley**
Draft a job description to hire professional IT services.

4. CONTRACT WITH SPRINGER

A proposal to renew our contract with Springer is being discussed. If we commit to a five-year contract, Springer offers to make old publications open access. We will need to see the full revised contract to make a decision, so this discussion is postponed.

5. PROPOSALS FOR EUROCRYPT 2027

There are two proposals for *Eurocrypt 2027*:

(1) In April 2027, at the Eindhoven University of Technology, or
(2) In May 2027, at a convention center in Rotterdam.

Both teams will be asked to update their proposals with comparable numbers of participants and sponsorship, and the Board will vote in a future meeting.

6. CO-EDITORS IN CHIEF OF THE IACR COMMUNICATIONS IN CRYPTOLOGY

In June 2022, it was suggested that Co-Editors in Chief of the IACR Communications in Cryptology (CiC) would be appointed for four-year-long terms, designed to stagger with appointments every two years. The IACR Bylaws will be amended to formalize the appointment process and to make one of the Co-Editors a Board Member. In retrospect, four years may be too long a commitment: the Secretary will ask for the opinion of the current Co-Editors.

Action Point **3: Wesolowski**
Draft an amendment of the IACR Bylaws to formalize the role and appointment of the Co-Editors in Chief of the IACR Communications in Cryptology.

7. A SPONSORSHIP COMMITTEE

The Vice President is currently setting up a Sponsorship Committee, tasked with building and maintaining relationships with companies. So far, four people have volunteered for the committee: herself, Britta Hale, and Mariana Raykova. All three are from the US, so Bishop is now looking for volunteers from the rest of the world.

8. CODE OF CONDUCT AND RELATED DOCUMENTS

Bishop presents the next item on the agenda: she is starting to work on a unified Code of Conduct for all of our events. Currently, each conference has its own Code of Conduct. She reviews the current situation. For instance, for our General Conferences, the General Chair Guidelines include a template for the Code of Conduct with blanks to be filled depending on the event.

LaMacchia suggests that we could have a global Code of Conduct for all IACR-related activities (e.g., journal submissions, schools, etc.). This could be considered, although many code-of-conduct issues are specific to in-person events.

Bishop will collect input from General Chairs and Program Chairs and bring it back to the Board. One particular issue she would like to address is how to handle situations where General Chairs or other key actors have a

conflict of interest in a conflict.

Action Point **4: Bishop**
Draft a unified Code of Conduct for all IACR events.

9. Publication and Conference Model

The last item on the agenda concerns the publication and conference model. There is increasing interest in moving to a hybrid model of publication for our General Conferences. It raises a number of questions:

- Would there be a single pipeline for all three conferences, or independent submissions?
- How should papers be linked to presentations? Should we insist on having a presentation for each accepted paper?
- If we opt for a unified pipeline, how would papers be assigned to a conference? If we let people choose, would that negatively impact some of the conferences?

Regarding the conference model, we need both a short-term and long-term plan to handle growth. Venues are chosen years in advance, and venues cannot accommodate an arbitrary number of tracks. For the next few years, we can commit to three tracks per conference. To compensate for the growth, we can consider shorter talks, even down to 10 minutes if necessary.

This solution might not scale well, and alternative solutions need to be discussed. A committee is formed to work on concrete questions to ask at the Assembly (*Crypto 2024*). LaMacchia, McCurley, Preneel, Rodríguez-Henríquez, Schwabe, Bishop, and Abdalla join this committee and will meet on Tuesday at 15:30.

10. Closing Matters

The President closes the meeting.