MINUTES IACR BOARD MEETING *VIRTUAL-01 2024*

16 JANUARY 2024

1. Opening Matters

1.1. **Welcome, roll of attendees, identification of proxies.** At 15:04 UTC the President opens the meeting and briefly goes around for an introductory round, confirming attendees and establishing who is holding proxies. The President welcomes the new Board members María Naya-Plasencia, Francisco Rodríguez-Henríquez, Dario Fiore, and Joseph Liu. The President gives a rapid overview of how Board meetings usually go, the typical structure of the agenda, and how voting works.

There are 21 full time attendees with the following proxies: Halevi holds Bishop's proxy, Lepoint holds Lysyanskaya's proxy, Yang holds Schwabe's proxy, Poettering holds Hesse's proxy (when absent), Guo holds Liu's proxy.

1.1.1. *Roll of Attendees.*

Attendees (Elected). Michel Abdalla (President 2023-2025); Brian LaMacchia (Treasurer 2023-2025); Benjamin Wesolowski (Secretary 2023-2025); Jian Guo (Director 2022-2024); Shai Halevi (Director 2023-2025); María Naya-Plasencia (Director 2024-2026); Bart Preneel (Director 2023-2025, Program Chair Contact); Francisco Rodríguez-Henríquez (Director 2024-2026); Bo-Yin Yang (Director 2022-2024); Moti Yung (Director 2021-2023, *PKC* Steering Committee);

Attendees (Appointed). Dario Fiore (Eurocrypt 2025 General Chair (2024-2025)); Julia Hesse (*Eurocrypt 2024* General Chair (2023-2024)); Tancrède Lepoint (*Crypto 2024* General Chair (2023-2024)); Bertram Poettering (Membership Secretary 2023-2025); Vincent Rijmen (Journal of Cryptology Editor-in-Chief 2024-2026);

Attendees (Representatives and Others). Gregor Leander (*FSE* Steering Committee).

Absentees (Elected). Allison Bishop (Vice President 2023-2025); Anna Lysyanskaya (Director 2022-2024); Peter Schwabe (Director 2023-2025);

Absentees (Appointed). Foteini Baldimtsi (Communications Secretary 2023-2025); Joseph Liu (Asiacrypt 2025 General Chair (2024-2025)); Bimal Roy (*Asiacrypt 2024* General Chair 2023-2024);

Absentees (Representatives and Others). Hilarie Orman (Archivist); Kevin McCurley (Database Administrator); Tal Rabin (Code-of-Conduct Liaison); Yu Yu (Webmaster);

1.2. **Approve minutes from last BoD virtual meeting.** The President thanks the Secretary for the completion of the minutes which have been shared before the current Board Meeting. The President calls for a vote to approve the minutes of the previous meeting.

Decision 1 (unanimous)**.** *The Board approves the Minutes of the IACR Board Meeting Virtual-11 2023.*

2. Conferences

2.1. **Update on conferences.** Leander and Rijmen report on *FSE*. All is going fine, we have a venue, finances and contracts are being handled with care. LaMacchia reports on *RWC*. Registrations have opened, and acceptance notices for talks will be sent out soon. A pattern has been noticed in the cohort of students asking for travel stipends: they often come from the same groups. We are in a situation where "people who know about stipends ask for stipends".

Hesse reports on *Eurocrypt*. It is going fine. Hesse asks how the currency gap should be handled: the USD/CHF exchange rate has shifted significantly since the original budget, to our disadvantage. It currently looks like costs are going to be 16% higher than budgeted. The Treasurer explains that there is currently no mechanism to manage currency risk; we do not hedge on currency. The registration fee is set at the time we have to (close to opening registrations), and fluctuations *after* that point are absorbed by IACR. Therefore, the usual solution to the problem at hand is to fix a higher registration fee than anticipated in the budget. Concern is expressed that higher registration fees may decrease attendance, worsening the issue. Another solution would be to compensate with more sponsorship income.

Yung and Lepoint give a brief report on *PKC* and *Crypto*: they are on track.

3. Topics

3.1. **Review of open tasks.** The Secretary has compiled a list of open tasks from 2023.

3.1.1. *Page limit policy.* Early 2023, the Board discussed the page limit at the general conferences. There seemed to be a consensus to exclude references from the page limit. Recent calls for papers (*Asiacrypt 2023*, *Eurocrypt 2024*, *Crypto 2024*) have implemented that, but with varying page limits (27 or 30 pages). Should we agree on a limit, and include it in the Guidelines for Program Chairs?

Leander, as program co-chair of *Eurocrypt 2024* has appreciated the freedom to choose the limit. Abdalla notes that it may still be good to fix a standard for the general conferences for consistency and predictability (authors preparing a submission before publication of the call for papers). By a show of hands, a limit of 28 pages (excluding references) is the most popular choice.

3.1.2. *Co-location of events.* To reduce the complexity, cost, and environmental impact of traveling, the Board has proposed to encourage co-location of events (for instance, an area conference and a general conference happening nearby in consecutive weeks). We have not yet gathered feedback from the steering committees of area conferences on the matter.

Action Point **1:**
Get feedback from the steering committees of area conferences on how to best implement co-location of events.

3.1.3. *Code of conduct.* The Ethics Committee was tasked with drafting a new IACR-level code of conduct. This is still in progress.

3.1.4. *Names for sponsorship committee.* It was suggested to create a Sponsorship Committee, tasked with building and maintaining relationships with companies. It was decided to investigate whether some IACR members would be interested in joining such a committee. Some people have been contacted, and we are waiting for their feedback.

3.1.5. *Statements and petitions.* Statements and petitions are occasionally published on the IACR website. It was noted that the nature of these statements is not explained on the website. It may be difficult to interpret them, or to understand why the IACR is publishing them. The Board decided to update the website to include an explanation of the nature and purpose of statements.

The Board agrees that, before drafting, further discussion is needed to decide on the message we want the explanation to convey.

3.1.6. *Other longer-term matters.* The Secretary reviews other open matters that will require further discussion and action: staffing (McCurley being almost singlehandedly maintaining a large part of our infrastructure), and the publication model.

3.2. **Review of committees.** The President introduces the next item on the agenda: reviewing the composition of existing committees.

3.2.1. *Audit and Election Committees.* There are no changes to discuss for the Audit and Election Committees.

3.2.2. *Investment Committee.* The Treasurer reports on the Investment Committee. The committee has put in place investment policies which the Treasurer has been following since then. This initial work being done, the committee has not been meeting regularly. He suggests yearly meetings may prove beneficial. He proposes to keep its current composition.

3.2.3. *Ethics Committee.* The Ethics Committee currently requires its members to be Board members. It is suggested to change the guidelines to allow for non-Board members. Bishop has drafted an update of the relevant section of the guidelines, sent by email ahead of the meeting. It is noted that other changes to the guidelines are needed, in particular to align them with the IACR bylaws (regarding disciplinary measures). Therefore the vote to change the guidelines is postponed until a complete update is drafted.

Action Point **2:**
Draft an update of the Ethics Committee guidelines compatible with the IACR bylaws.

3.2.4. *Schools Committee.* The Schools Committee is currently chaired by Lepoint. Lepoint wishes to step down at the next opportunity. The next chair has to be a Board member.

There is a position to fill, and Lepoint calls for volunteers. Rodríguez-Henríquez offers to join the Schools Committee.

3.2.5. *Test-Of-Time Committee.* The Test-Of-Time Committee currently invites Program Chairs from upcoming conferences to join. This can pose a challenge as Program Chairs are typically very busy. Should this be changed? One idea could be to invite Program Chairs from *past* conferences (rather than upcoming).

Action Point **3:**
Update the IACR website with the current composition of committees.

4. Closing Matters

The President announces that we will be electing the Program Chairs of *Eurocrypt*, *Crypto* and *Asiacrypt* in March, April and May respectively.

Naya-Plasencia suggests that we discuss the matter of the publication model soon. While such long-term matters are usually discussed at Strategic Meetings, we can still dedicate a Virtual Meeting to it, for faster progress. The February meeting may be suitable.

The President closes the meeting officially at 16:45 UTC.