MINUTES IACR BOARD MEETING *VIRTUAL-02 2024*

20 FEBRUARY 2024

1. Opening Matters

1.1. **Welcome, roll of attendees, identification of proxies.** At 21:06 UTC 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 with the following proxies: Bishop holds Lepoint's proxy, Yang (and when absent, Naya-Plasencia) holds Guo's proxy, LaMacchia holds Yang's proxy (when absent), Preneel holds Rijmen's proxy.

1.1.1. *Roll of Attendees.*

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

Attendees (Appointed). Foteini Baldimtsi (Communications Secretary 2023-2025); Dario Fiore (Eurocrypt 2025 General Chair (2024-2025)); Julia Hesse (*Eurocrypt 2024* General Chair (2023-2024)); Joseph Liu (Asiacrypt 2025 General Chair (2024-2025)); Bertram Poettering (Membership Secretary 2023-2025);

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

Absentees (Elected). Jian Guo (Director 2022-2024);

Absentees (Appointed). Tancrède Lepoint (*Crypto 2024* General Chair (2023-2024)); Vincent Rijmen (Journal of Cryptology Editor-in-Chief 2024-2026); Bimal Roy (*Asiacrypt 2024* General Chair 2023-2024);

Absentees (Representatives and Others). Hilarie Orman (Archivist); 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-01 2024.*

2. Policy around accepting credit cards for sponsorship payments

The Treasurer introduces the first topic of the meeting. Sponsors of IACR conferences occasionally ask to pay sponsorship by credit card. So far, we have not allowed that, and require sponsors to pay through wire transfer. Indeed, credit card transfers incur a processing fee of 4% (or more) of the transferred amount.

Sponsorship typically has tiers, say, 10000 USD to be a *Gold sponsor*, corresponding to pre-specified benefits. If the sponsor pays 10000 USD by credit card, and IACR pays the processing fee, then IACR loses 400 USD. The Treasurer proposes to formally implement the following policy: if a sponsor asks to pay by credit card, we can accept, but the resulting extra cost (e.g., 4%) must be added to the price of the sponsorship tier.

The Board raises a few questions, and LaMacchia provides clarification:

- Should we advertise this option on the call for sponsorship? No, we probably do not want to advertise this option, as we do not want to encourage credit card payments. However, we should explicitly state that the amount for each tier assumes a wire transfer payment. Sponsors should be aware that the payment medium may add an extra cost.
- In some cases, the call for sponsorship may not have a tier system. Then, it makes no sense to add an extra 4%: we can only accept the exact amount proposed by the sponsor, and try to convince them to pay by wire transfer. If they insist on paying by credit card, IACR will pay the fee.

- It seems only few sponsors ever ask to pay by credit card; do we need a policy? Yes, if only to ensure consistency across all of our events. Also, a large company with a corporate card may soon value the convenience of paying by credit card. So if we don't have consistent policy to enforce the extra 4%, we may end up losing money from such sponsors.

The President calls for a vote.

Decision 2 (unanimous)**.** *The Board approves the proposed policy: we may accept alternative payment methods from sponsors, but the resulting extra cost must be added to the price of each sponsorship tier.*

3. Discussion on publication and conference models

The Vice President introduces the second topic of the meeting, which can be divided into two aspects:

(1) The model of the general IACR conferences, and the proposal to include posters.
(2) The publication model for these conferences, and what we have learned so far about the publishing workflow for the new journal.

We start by discussing the first point: the conference experience. Schwabe recalls the main ideas of the proposal *Posters by default: a proposal for IACR conferences* (first discussed at the *Crypto 2023 Strategic Meeting*). Our general conferences have an evident scaling issue: the number of submissions is growing steadily, and to preserve (i) the acceptance rate and (ii) the "one paper = one talk" tradition, the IACR conferences have increased the number of tracks in the program. We are now at 3 tracks, and the numbers keep growing. Venues with multiple very large rooms are harder to find and more expensive. Confronted to a similar situation, neighboring communities (Usenix, CCS) are moving to poster sessions.

The Board discusses the issue, raising the following points.

- The problem we are facing concerns the structure of our conferences. Through them, we are directing people's attention, allocating time, exposition. Presentation slots, posters, recorded talks, are several ways to achieve that.
- The driving concern behind the proposal *Posters by default* was to design an enjoyable conference, and to give time for people to meet and interact. If posters are the default option, Program Chairs have more freedom to curate an enjoyable program, with fewer, longer, high quality talks, gathering more people in the same room.
- Giving a talk can be important for younger researchers (it is formative, and it gives visibility). Possible solutions include (i) pre-recorded talks (ii) sessions of "lightning talks" (iii) prioritizing young researchers for the few remaining talk slots in the program.
- Some Board Members express their satisfaction with the current system: can we not simply continue with the increasing number of tracks? This would pose significant challenges. Venues allowing for many tracks can get very expensive (and rare). It complicates the organisation, and affects the price of the conference, hence its accessibility.
- Bishop reports on some informal feedback from the community (gathered at the Crypto 2023 membership meeting) on the question: which is more important between
  (1) keeping acceptance rates up,
  (2) keeping costs and numbers of tracks down, or
  (3) maintaining the "one paper = one talk" practice.
  By show of hands, talk slots are deemed least important.
- Bishop reports on a survey for student NSF support recipients after the conference. There were 17 responses. One question was: "What was most valuable to you at Crypto?", and the choices were
  (1) networking with students from other institutions,
  (2) networking with senior researchers and industry,
  (3) attending talks,
  (4) presenting a talk, and
  (5) other.
  For most valuable, about 2/3 of the responses said networking with other students, and about 1/3 said networking with senior researchers and industry. For least valuable, about 1/2 said attending the talks. The other half was somewhat split.
- Should we wait and observe how neighboring communities transition to posters? On one hand, it would give us the opportunity to learn from them and possibly avoid mistakes. On the other hand, the issue worsens every year, and we may need to be more proactive. In any case, we can already get in touch with them: they must have discussed the matter thoroughly, and they reached a conclusion; we can learn from that.

- If some papers get a poster, and others get a talk slot, this may create a two-tier system. The Board discusses whether having two tiers is a problem. On one hand, it could simply reflect the fact that some papers deserve more attention than others. On the other hand, we do not want poster papers to be denigrated, to the points where the "Crypto/Eurocrypt/Asiacrypt" stamp loses prestige. The discussion continues with ideas to mitigate this concern. There are two levers: the number of papers which get a presentation slot (possibly very few: best papers, honorable mentions, maybe *area chairs* select the best of each "area"...), and how they are selected (quality of the paper, expected quality of the talk, random choice...).

The discussion moves to the second point: the publication flow. McCurley recalls that publishing is essentially a three-steps process: (i) submission and reviewing, (ii) copy editing and production, and (iii) indexing and web hosting. Four different combinations of systems are used by the *Journal of Cryptology*, the *IACR Communications in Cryptology*, the journals *ToSC* and *TCHES*, and the other IACR conferences.

The Board discussed the possibility to move the IACR general conferences to a "journal first" model. For instance, at the *Eurocrypt 2023 Strategic Meeting*, the following proposal was discussed: instead of being submitted to *Asiacrypt*, *Crypto* or *Eurocrypt*, articles would be submitted to a single journal; accepted papers would then be presented at one of the three venues following some rule to be determined.

The following points are raised.

- Changing the publication from *conference proceedings* to *journal first* has consequences. Indexing distinguishes between conferences and journals. The IACR conferences would drop out of the conference ranking systems. Changing the type of publication (or changing the name, or leaving Springer) implies losing the bibliometric reputation built with the current system. We would have to rebuild that.
- It is observed that we can make substantial changes to the system without affecting the actual publication, if that is a problem. Indeed, we could change the submission mechanisms and reviewing flow, while still publishing the accepted articles in the same conference proceedings. In particular, the questions of *self-publishing* and *journal first* are independent.

McCurley concludes that we need to clarify what problem we are trying to solve with these changes.

> Action Point **1:**
> Organise a working group on the publication and conference models, in preparation for the next strategic meeting.

Bishop, Naya-Plasencia, Wesolowski, McCurley, and Schwabe volunteer for the working group. Bishop volunteers to take the lead.

4. Closing Matters

The President closes the meeting officially at 22:56 UTC.