MINUTES IACR BOARD MEETING *VIRTUAL-09 2023*

21 SEPTEMBER 2023

1. Opening Matters

1.1. **Welcome, roll of attendees, identification of proxies.** At 16:04 UTC Abdalla 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 Abdalla's proxy (when absent), Halevi (then Hesse) holds Lysyanskaya's proxy, Yang holds Guo's proxy (when absent), Hale holds Lepoint's proxy (when absent), Yang holds Schwabe's proxy, Bishop holds Baldimtsi's proxy, Poettering holds Hesse's proxy (when absent), Preneel holds Rijmen's proxy, Abdalla holds Stehlé'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); Masayuki Abe (Director 2021-2023); Jian Guo (Director 2022-2024); Shai Halevi (Director 2023-2025); Tancrède Lepoint (Director 2021-2023, *Crypto 2024* General Chair (2023-2024)); Bart Preneel (Director 2023-2025, *FSE* Steering Committee, Program Chair Contact); Bo-Yin Yang (Director 2022-2024); Moti Yung (Director 2021-2023, *PKC* Steering Committee);

Attendees (Appointed). Britta Hale (*Crypto 2023* General Chair (2022-2023)); Julia Hesse (*Eurocrypt 2024* General Chair (2023-2024)); Bertram Poettering (Membership Secretary 2023-2025); Fangguo Zhang (*Asiacrypt 2023* General Chair (2022-2023));

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

Absentees (Appointed). Foteini Baldimtsi (Communications Secretary 2023-2025); Vincent Rijmen (Journal of Cryptology Editor-in-Chief 2021-2023); Bimal Roy (*Asiacrypt 2024* General Chair 2023-2024); Damien Stehlé (*Eurocrypt 2023* General Chair (2022-2023));

Absentees (Representatives and Others). Kevin McCurley (Database Administrator); 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-08 2023.*

2. Conferences

2.1. **Update on conferences.** Hale reports on *Crypto*. All 536 participants survived the hurricanes and earthquakes. The conference went mostly according to plan. Schwabe shared information about how *CHES 2023* went by email ahead of the meeting, mentioning that it was a big success with significant attendance. Yang reports on *TCC*, mentioning that registration is now open and on-campus housing has been arranged. Several stipends have already been distributed, and there are currently three registered participants. Zhang provides an update on Asiacrypt, stating that the final budget needs approval before opening registrations. Preneel reports on *FSE*, confirming that everything is on track. LaMacchia reports on *RWC*, stating that everything is on track. He checked out the venue in person, and believes it will work nicely. Abdalla reports on *PKC* and the possibility of reducing student registration fees with minor adjustments. A vote by email may be called soon.

2.2. **Update on Eurocrypt 2024.** Hesse reports on the progress of Eurocrypt 2024. The workshops will be held at ETH rent-free. The submission server is now online. A tax consultant has sent documentation. There have been some positive responses to the first round of sponsorship requests.

Hesse notes a loss compared to the proposed budget due to the fluctuation of the CHF/USD exchange rate. To offset this loss, she considers cancelling the reception venue. Poettering raised the concern that participants would still need to eat on Sunday, and by canceling the reception, we would only move the cost from the registration fee to individual dinners (which, in Zurich, is expensive anyway). Hesse clarifies that cancelling the reception venue

does not necessarily mean cancelling the reception altogether. It could be replaced by a simpler, less formal one, possibly held at ETH. She adds that the venue has a cancellation penalty.

2.3. **Test of Time Award committee appointment.** The Board needs to appoint a new member for the Test of Time Award committee. Four candidates have been nominated, and each is presented by the board member who nominated them. The president calls for a vote.

Decision 2. *The new Test of Time Award committee member is selected, as well as a runner-up in case the first declines the invitation. [Update: Jean-Sebastien Coron is the new Test of Time Award committee member.]*

2.4. **Discussion on concrete steps related to recent diversity proposals.** Bishop initiates a discussion on several topics related to recent diversity proposals.

Visa Letters. The proposal mentions easing the process of issuing visa letters. This process cannot be fully automated, to prevent abuse of the system. Bishop suggests centralising the visa letter issuance within IACR, allowing people to contact an IACR representative independently of the general chairs of each conference. A central contact point may ease the process, but LaMacchia raises the question of whether some countries require the letter to be issued by someone from that country. Instead, Hale suggests publishing more information on the main IACR website with clear instructions like "email the general chair of your event." The best solution might simply be to ensure that general chairs are appointed on time and that this information is available early to potential participants. Appointements are done quite early, but the information has not always been easy to find well in advance.

Communities/groups/social networking on the IACR website. Next, the board discusses the possibility of helping communities and groups like QueerCrypt and WinC with their communication. The IACR website could provide a listing of such groups, information on upcoming events and mailing lists. Concern is raised about moderation of such a listing and services.

Dedicated IACR person for sponsorship. Bishop raises the idea of having an IACR person dedicated to sponsorship, focusing on building and maintaining relationships with companies. More generally, there may be a need for a more strategic approach to sponsorship. Yung suggested that the responsibilities might be too extensive for one person and recommended forming a committee. It is pointed out that some sub-communities might be protective of their sponsor relationships and may not choose to centralise. Rather than a full centralisation, Halevi suggests that it should be a resource available to general chairs, as they often lack experience in searching for sponsors. Providing useful information, templates, contacts, introducing people, and general advice. A sponsorship coordinator (or committee) would maintain an information repository and facilitate connections. Bishop recommends moving forward with finding potential committee members. Former general chairs, who have experience with sponsors, may be good candidates.

> Action Point **1:** *(no time set)*:
> Generate a list of potential candidates for a sponsorship committee.

2.5. **Follow-up on Proposal for the IACR to Join the CRA.** LaMacchia provides an update on the proposal to have the IACR join the CRA (Computing Research Association). A concern that was raised in that the CRA is North American while the IACR is international; how is the cost of a CRA membership justified to members outside North America? LaMacchia discussed the matter with an IEEE representative at CRA, who mentioned that their involvement with the CRA is part of a global portfolio. The question of European or Asian equivalents to the CRA is raised, and ERCIM is mentioned, with uncertainty about the nature of its activities.

Additional costs are discussed, particularly related to travel for meetings. Meetings are typically held in the US, either DC or the West coast.

To cover for the fee and additional costs, two possibilities are presented: increasing the IACR membership fees (which has not happened for a while), or funding from local events. Registration to events in North America could contribute to the CRA membership costs.

LaMacchia will circulate a summary of the pros and cons for a vote by email or discussion at the next meeting.

3. Closing Matters

The President closes the meeting officially at 17:45 UTC.