

MINUTES IACR BOARD MEETING *VIRTUAL-10 2023*

18 OCTOBER 2023

1. OPENING MATTERS

1.1. Welcome, roll of attendees, identification of proxies. At 16:04 UTC LaMacchia (acting as the President's proxy) 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: LaMacchia holds Abdalla's proxy (when absent), Lysyanskaya holds Hale's and Hesse'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); Masayuki Abe (Director 2021-2023); Jian Guo (Director 2022-2024); Shai Halevi (Director 2023-2025); Tancrede Lepoint (Director 2021-2023, *Crypto 2024* General Chair (2023-2024)); Anna Lysyanskaya (Director 2022-2024); Bart Preneel (Director 2023-2025, *FSE* Steering Committee, Program Chair Contact); Peter Schwabe (Director 2023-2025); Bo-Yin Yang (Director 2022-2024); Moti Yung (Director 2021-2023, *PKC* Steering Committee);

Attendees (Appointed). Bertram Poettering (Membership Secretary 2023-2025); Damien Stehlé (*Eurocrypt 2023* General Chair (2022-2023)); Fangguo Zhang (*Asiacrypt 2023* General Chair (2022-2023));

Attendees (Representatives and Others). Tal Malkin, Mariana Raykva and Edoardo Persichetti have joined relevant parts of the meeting.

Absentees (Elected). Allison Bishop (Vice President 2023-2025);

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

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. LaMacchia thanks the Secretary for the completion of the minutes which have been shared before the current Board Meeting. LaMacchia 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-09 2023.*

2. CONFERENCES

2.1. RWC 2025 proposal. Mariana Raykova has joined the meeting to discuss the *RWC 2025* proposal. The proposal has been sent to the Board by email ahead of the meeting. The event would happen in Sofia in 2025, hosted by the new institute for computer science INSAIT. Raykova presents the venue, which can easily accommodate 800 people. The anticipated registration fees would be close to previous years.

LaMacchia notes that *Eurocrypt 2015* happened in Sofia (although at a different venue), and it went well. Some details on the proposal are discussed further (the possibility for hotel deals, the registration fee). LaMacchia calls for a vote on the proposal.

Decision 2 (unanimous). *The proposal to host RWC 2025 in Sofia is approved.*

2.2. Update on conferences. Yang reports on *TCC 2023*. The organisation is moving forward, and sponsorship has been higher than usual. There are plans to give a cancellation waiver to anyone affected by the recent events in the Middle East. There are currently 125 registered participants, which is about average for *TCC*.

Zhang reports on *Asiacrypt 2023*. Registration has just opened, and there are currently 30 registered participants. LaMacchia reports on *RWC 2024* in Toronto. Catering, hotel deals, and sponsorships are all on track. Preneel reports that everything is on track for *FSE 2024*. Yung reports on *PKC 2024* in Sydney. The submission deadline has just passed, all is on track for the reviewing process. Lepoint reports on *Crypto 2024*: the website is online, the call for papers is out, and the beach is booked.

3. TOPICS

3.1. IACR elections. Halevi notifies the board that he will try to update the guidelines for the IACR elections, to modernise the process.

While on that topic, LaMacchia asks for information about the recent issue with Helios: IACR members all received several identical emails from the Helios system about the IACR 2023 Board of Directors Elections. The explanation seems to come from a bug in Helios: a first email was created, but nothing happened. The following day, as still nothing had happened, the email was created again, several times, with no apparent result. They then all went through at the same time.

3.2. New coeditor of the Cryptology ePrint Archive. Lepoint wishes to step down from his position as coeditor of the Cryptology ePrint Archive. Lepoint nominates Matthias J. Kannwischer as a candidate for this position. Two other board members vouch for him and his reliability, and LaMacchia calls for a vote.

Decision 3 (unanimous). *Kannwischer is the new coeditor of the Cryptology ePrint Archive, effective today.*

3.3. Update to the code of conduct. Schwabe presents the following matter. For *RWC*, one of the sponsors asked whether the code of conduct for the event includes any explicit mention of diversity and inclusion. It currently does not, and the Board may wish to work on an update of the code of conduct.

Abdalla notes that the code of conducts are currently per-conference (usually reproduced from the template provided in the General Chair Guidelines; modifications are allowed, subject to approval of the Board). However, it has been proposed to replace it with an IACR-level code of conduct. A global code of conduct could cover not only conference participation, but also matters related to publication or membership.

The consensus arising from this discussion is that the code of conduct may indeed need to be modernised. It is proposed for the Ethics Committee to draft it.

Action Point 1:

Commission the Ethics Committee to draft a new code of conduct.

3.4. Eurocrypt 2026. Edoardo Persichetti has joined the Board meeting to present the proposal to host *Eurocrypt 2026* in Rome. The budget is drafted for an estimated 700 participants, and two possible venues are presented.

The main challenge is the triple-track constraint: while there are many large venues, most only have a single big auditorium. The first option has rooms of size 734, 250 and 150. Having a track in a room as small as 150 seats is a concern, as distribution of participants across tracks is hard to predict. The second option has much bigger rooms, but is noticeably more expensive. It is noted that ensuring that there is room for everyone has high priority.

Discussions follow on details in the budget (regarding VAT, or EUR/USD rates). Persichetti proposes to reach back to the board with updated estimates.

3.5. IACR statement on recent events in Israel. A group of Board members and IACR members have drafted a possible statement for IACR to adopt regarding the October 7 terrorist attack on Israel. The following draft was sent to the board ahead of the meeting:

The IACR strongly condemns the atrocities perpetrated by Hamas against Israel. We are outraged and horrified by this dreadful assault on civilians: Israelis of all religions, ages, and backgrounds; tourists; and foreign workers. We stand in solidarity with the people of Israel. Our heartfelt sympathy and support goes out to our members in Israel, and all those who are suffering the results of that attack.

Several Board members express agreement that a statement of this nature should be adopted. Still, some concerns are expressed about the proposed draft. It is noted that the whole conflict has since shifted, and there is also tremendous suffering in Gaza from the reaction to the attack. The statement should not appear like IACR is taking sides. Authors of the draft reassure the Board that they share this sentiment, and the last sentence is meant to express support to *all* those suffering from the events, also outside Israel. Modifications are suggested to make this point clearer, notably by (1) explicitly writing “members everywhere” in that sentence, and (2) mark a separation between the first two sentences (which refer specifically to the October 7 attack which triggered the dramatic chain of events) and the last one (about ongoing consequences everywhere).

Some concerns are raised about how parts of the statement could still be misconstrued. After some interactive discussion and wordsmithing, a vote is called.

Decision 4. *The group of members who submitted the draft are empowered to incorporate the feedback from the board and publish the statement.*

4. CLOSING MATTERS

The President closes the meeting officially at 18:14 UTC.