

MINUTES IACR BOARD MEETING *VIRTUAL-04 2024*

16 APRIL 2024

1. OPENING MATTERS

1.1. Welcome, roll of attendees, identification of proxies. At 14:06 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: Abdalla holds Fiore's proxy, Hesse holds Poettering's proxy, Guo holds Liu's proxy, Lysyanskaya's holds Baldimtsi's proxy, Preneel holds Lepoint's and Rijmen's proxy (when absent).

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); Jian Guo (Director 2022-2024); 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). Julia Hesse (*Eurocrypt 2024* General Chair (2023-2024)); Tancrède Lepoint (*Crypto 2024* General Chair (2023-2024)); Vincent Rijmen (Journal of Cryptology Editor-in-Chief 2024-2026);

Attendees (Representatives and Others). Gregor Leander (*FSE* Steering Committee); Kevin McCurley (Database Administrator); Tal Rabin (Code-of-conduct Liaison);

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

Absentees (Representatives and Others). Hilarie Orman (Archivist); 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-03 2024.*

2. CODE OF CONDUCT

2.1. Code of conduct: representatives at conferences. Rabin, the Code-of-Conduct Liaison, introduces the first topic of the meeting. She would like to appoint delegates to help her with the task of handling code-of-conduct matters at conferences. Such delegates would be appointed for a long term, forming a permanent pool of trained individuals to draw from, ensuring that each IACR event has at least three (depending on the size of the event) qualified points of contact available on-site.

Having such delegates would prevent issues that occurred at recent events where there were no (or too few) properly appointed points of contact for code-of-conduct matters.

A point is raised that this pool of code-of-conduct delegates should be mostly independent from the IACR Board of Directors and the Ethics Committee. Nevertheless, the event's General Chairs, the IACR President, and the Chair of the Ethics Committee, will still serve as points of contact.

It is proposed that the Code-of-Conduct Liaison (currently Rabin) be given the authority to appoint these delegates. The president calls for a vote.

Decision 2 (unanimous). *The Board approves the following proposal: the Code-of-Conduct Liaison is given the authority to appoint delegates to address code-of-conduct reports at conferences.*

These delegates will be listed on the IACR website, and delegates on duty at an event will be listed on the event's website.

Action Point 1:

Ask for volunteers for these code-of-conduct delegate positions at the next Membership Meeting.

Rabin adds that the pool of delegates should have at least one senior person. She calls for ideas of people who could fulfill this position: a senior person (not from the Board) with a strong and positive reputation in the community.

Lepoint raises another point: there are currently no guidelines for the Code-of-Conduct Liaison. We had already planned to revise the guidelines concerning the code of conduct itself (currently only discussed in the General Chair Guidelines), and we should take this opportunity to formalize the role of the Code-of-Conduct Liaison. This will ensure continuity when Rabin leaves this role.

2.2. Code of conduct: clarification about conflicts of interest. Rabin introduces the next point: the current guidelines for the code of conduct do not anticipate situations where the contact person has a conflict of interest in a code-of-conduct matter. She adds that with three on-site contact persons, there should always be at least one without a conflict. But what about a situation where herself, the Code-of-Conduct Liaison, is conflicted?

Action Point 2:

(Re)write the Code-of-conduct Guidelines to address points discussed above: formalizing the roles of the Code-of-Conduct Liaison and delegates, and how to handle conflicts of interest.

3. CONFERENCES

3.1. Proposal for CHES 2025. A proposal to host *CHES 2025* in Kuala Lumpur, Malaysia, was presented. A preliminary discussion about hosting *CHES 2025* in Malaysia took place during the November 2023 Board Meeting. Because of travel restrictions to the country, the Board requested the conference to facilitate online participation. A formal proposal was sent to the Board ahead of the current meeting, and the President calls for a vote.

Decision 3 (unanimous). *The Board approved the proposal to host CHES 2025 in Kuala Lumpur, Malaysia.*

3.2. Proposal for RWC 2026. LaMacchia presents a proposal to host *RWC 2026* in Taipei, Taiwan. The proposal was sent to the Board ahead of the meeting. The IACR already has experience running conferences in Taipei. LaMacchia and Yang visited the venue: the space is configurable and easy to scale to up to 1000 participants. Costs are reasonable, on par with *RWC 2025* in Sofia. Finances would be handled through Academia Sinica, as was done for *TCC 2023*.

LaMacchia emphasizes that the RWC Steering Committee is committed to hosting the conference on a three-year rotation: Europe-Asia-America.

Decision 4 (unanimous). *The Board approved the proposal to host RWC 2026 in Taipei, Taiwan.*

3.3. Planning of future conference editions. The next topic on the agenda concerns the planning of future conference editions. We need to revise our process for selecting dates. We have many events, and they sometimes conflict with one another or with events of neighboring communities. The President proposes to postpone this discussion to the upcoming Strategic Meeting.

4. TOPICS

4.1. Co-Editors-in-Chief for TCHES 2025. The CHES Steering Committee has submitted two names for Co-Editors-in-Chief for TCHES 2025: Debdeep Mukhopadhyay and Michael Hutter. Schwabe presents them briefly, and the President calls for a vote.

Decision 5 (unanimous). *Debdeep Mukhopadhyay and Michael Hutter are appointed TCHES 2025 Co-Editors-in-Chief.*

4.2. Follow-up on the IACR statement and policy for future statements. The President introduces the next topic: the IACR Statement on the war in Gaza published on October 18, 2023. The President raises two questions:

- (1) Should we amend (or withdraw) the original statement, or publish a new statement to account for the evolution of the situation, and insist that the IACR is horrified by the immense suffering on all sides of the conflict?
- (2) Should the IACR keep issuing statements on similar matters, or restrict to issues directly related to our scientific expertise and mission?

A discussion ensues. Regarding the first point, only few voices advocate for the withdrawal of the original statement. The majority agrees with the proposal of amending it, raising the following points:

- The sentiment motivating the original statement is in line with the values of the community. Withdrawing it would send the wrong message.
- The statement is not meant to be political, but an expression of sympathy to suffering members of the community. If any part of it was perceived differently, an amendment should clarify it.
- An amendment would be a chance to ensure every member feels properly represented, especially following the evolution of the situation in Gaza.
- A point is made that it is hard not to be political: even *not* reacting to such events could be perceived as a political stance.

Action Point 3:

Draft an amendment for the IACR Statement on the war in Gaza published on October 18, 2023.

Concerning the second point on future IACR Statements, the discussion raises the following points. No consensus or clear majority is reached, and the points below express individual opinions.

- A point is made that not issuing statements would be the easy way out, but our community has values to defend. While statements should be written with great care, there should not be a policy against it.
- IACR statements are not political, they are sympathy messages. In response, it is pointed out that some past statements are unambiguously political (like the statement condemning the US immigration ban, published on January 29, 2017).
- The Board could ask the membership for a mandate to keep issuing IACR Statements.
- The benefit for the community of issuing statements is called into question. On one hand it risks creating divides. On the other hand, it is an acknowledgement of situations affecting people in our community.
- A point is made that we are not qualified to comment (to assess, to choose the right words) on matters outside our field of expertise. Keeping up with events around the world will be a difficult task.
- It is raised that currently IACR lacks of open criteria to guide on what events and how IACR should respond to, so that events can be handled consistently, fairly, and timely.

As no consensus is reached, the Vice President proposes to continue the discussion at the *Eurocrypt 2024* Strategic Meeting.

5. CLOSING MATTERS

The President closes the meeting officially at 16:10 UTC.