MINUTES IACR BOARD MEETING *VIRTUAL-04 2026*

21 APRIL 2026

1. OPENING MATTERS

1.1. **Welcome, roll of attendees, identification of proxies.** At 14:04 UTC the President opens the meeting and briefly goes around for an introductory round, confirming attendees and establishing who is holding proxies.

There are 22 full time attendees with the following proxies: Halevi holds Lysyanskaya's proxy, Naya-Plasencia holds Standaert's proxy, Yang holds LaMacchia's proxy. Preneel holds Naya-Plasencia's proxy (when absent), Preneel holds Rijmen's proxy.

1.1.1. *Roll of Attendees.*

Attendees (Elected). Allison Bishop (President 2026-2028); Benjamin Wesolowski (Secretary 2026-2028); Jian Guo (Director 2025-2027); Shai Halevi (Director 2026-2028); María Naya-Plasencia (Director 2024-2026); Bart Preneel (Director 2026-2028, Program Chair Contact); Francisco Rodríguez-Henríquez (Director 2024-2026); Peter Schwabe (Director 2026-2028, *CHES* Steering Committee); Bo-Yin Yang (Director 2025-2027); Moti Yung (Director 2024-2026, *PKC* Steering Committee);

Attendees (Appointed). Man Ho Allen Au (Asiacrypt 2026 General Chair (2025-2026)); Tetsu Iwata (Asiacrypt 2027 General Chair (2026-2027)); Andreas Hülsing (*Eurocrypt 2027* General Chair (2026-2027)); Edoardo Persichetti (*Eurocrypt 2026* General Chair (2025-2026)); Mayank Varia (*Crypto 2026* General Chair (2025-2026));

Attendees (Representatives and Others). Gregor Leander (*FSE* Steering Committee); Kevin McCurley (Database Administrator); Kay McKelly (Web & software developer);

Absentees (Elected). François-Xavier Standaert, (Vice President 2026-2028); Brian LaMacchia (Treasurer 2026-2028, *RWC* Steering Committee); Anna Lysyanskaya (Director 2025-2027);

Absentees (Appointed). Foteini Baldimtsi (Communications Secretary 2023-2026); Joppe W. Bos (IACR Communications in Cryptology Editor-in-Chief); Vincent Rijmen (Journal of Cryptology Editor-in-Chief 2024-2026); Chitchanok Chuengsatiansup (Membership Secretary (2026-2028));

Absentees (Representatives and Others). Masayuki Abe (*Asiacrypt* Steering Committee); Tal Malkin (*TCC* Steering Committee); Hilarie Orman (Archivist); Tal Rabin (Code-of-conduct Liaison); Yu Yu (Webmaster);

1.2. **Approving minutes from previous meeting.** The President calls for a vote to approve the minutes of the meeting *Virtual-03 2026*.

Decision 1 (unanimous). *The Board approves the Minutes of the IACR Board Meetings Virtual-03 2026.*

2. UPDATE ON CONFERENCES

Persichetti reports on *Eurocrypt 2026*. There are currently more than 600 registrations, which is on target. The Board will hold the *Eurocrypt Strategic Meeting* on the Sunday before the event, at the same venue as the affiliated events. Bishop invites Board members to submit topics for inclusion in the agenda.

Persichetti also reports on *PKC 2026*. Registration opened a few days ago, and everything is on track.

Varia reports on *Crypto 2026*. There are five confirmed affiliated events. The number of accepted papers is expected to reach a new record, nearing the venue's capacity limits. However, this year, authors who cannot attend in person will have the option to give an *asynchronous* remote presentation, easing pressure on the in-person program. The increase in submissions appears to be offset by the proportion of authors declaring they will not attend in person.

Schwabe reports on *CHES 2026*. There are three confirmed affiliated events, and preparations are proceeding as planned.

Au reports on *Asiacrypt 2026*. The organizers are actively seeking additional sponsors, and the call for affiliated events will be published soon.

Preneel informs the Board that *RWC 2027* is scheduled for the same week as the *RSA Conference 2027*, with *Eurocrypt 2027* following the next week. *Eurocrypt 2027* is exceptionally early that year to take advantage of the availability of the TU/e campus during spring break. *FSE* is also scheduled for spring, resulting in a concentrated season of events. Preneel suggests that we rework the scheduling of future IACR events.

RWC and *Eurocrypt* are both planned years in advance, before the dates of the RSA Conference are made public. To prevent future conflicts, the Board could reach out to the RSA Conference organizers to coordinate schedules.

3. Update on guidelines and policies

The President calls for more volunteers to join the working groups on guidelines and policies, as discussed during the last Board Meeting. She requests that each working group be led by a Board Member, who may invite non-Board members (in particular former General Chairs or Program Chairs).

Halevi emphasizes that the policy on the use of AI is the most pressing issue. While those enthusiastic about AI technology may be more likely to volunteer, he stresses the importance of diverse opinions being represented in the working group.

4. A Proposal for an IACR Initiative for Cryptographic Pedagogy

Nadim Kobeissi has submitted a Proposal for an *IACR Initiative for Cryptographic Pedagogy* to the Board. The proposal includes:

- the maintenance of a registry of peer-reviewed pedagogical material,
- the organisation of an annual workshop, and
- the creation of awards for contributions in cryptographic pedagogy.

Board members express support for the initiative, noting that it aligns with a similar proposal received in 2025. Given this overlap, the Board is confident that a strong team of volunteers can now be assembled. Before taking any formal action, the Board will connect the authors of the two proposals.

5. Working groups on the change of model for publication and conferences

Naya-Plasencia provides a brief update on the progress of the working groups on the publication model. The draft is advancing well, and all Board members are invited to review and comment on it. The latest discussion focused on the possibility to submit *extended abstracts* to the journal, to preserve a publication practice valued by many members of the community.

Bishop adds that the proposal will be discussed further during the *Eurocrypt 2026 Strategic Meeting*.

6. Selection of Program Chairs for Eurocrypt 2028

The President recalls that we need to select the two Program Chairs for *Eurocrypt 2028*. Three people were nominated. Each candidate is presented by the Board Member who nominated them, and the President calls for a vote to select the first Program Chair.

Decision 2. *María Naya-Plasencia is appointed Eurocrypt 2028 Program Chair. [Naya-Plasencia has since accepted.]*

The President calls for a vote to select the second Program Chair.

Decision 3. *Martin Albrecht is appointed Eurocrypt 2028 Program Chair. [Albrecht has since accepted.]*

7. Closing Matters

The President closes the meeting officially at 15:01 UTC.