MINUTES IACR BOARD MEETING *VIRTUAL-08 2024*

14 AUGUST 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 Bishop's proxy, Yang holds Guo's proxy (when absent), Halevi holds Lysyanskaya's proxy (when absent), Preneel holds Naya-Plasencia's proxy, Yang holds Schwabe's proxy (when absent), Wesolowski holds Lepoint's proxy (when absent), Guo holds Liu's proxy, Preneel holds Rijmen's proxy.

1.1.1. *Roll of Attendees.*

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

Attendees (Appointed). Tancrède Lepoint (*Crypto 2024* General Chair (2023-2024)); Bertram Poettering (Membership Secretary 2023-2025);

Attendees (Representatives and Others). Kevin McCurley (Database Administrator);

Absentees (Elected). Allison Bishop (Vice President 2023-2025); María Naya-Plasencia (Director 2024-2026);

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

Absentees (Representatives and Others). Gregor Leander (*FSE* Steering Committee); Tal Malkin (*TCC* Steering Committee); Mitsuru Matsui (*Asiacrypt* Steering Committee); 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 completing the minutes which have been shared before the current Board Meeting. The Secretary reports on two minor modifications to the draft of the minutes. The President calls for a vote to approve the minutes of the previous meeting, subject to these modifications.

Decision 1 (unanimous)**.** *The Board approves the Minutes of the IACR Board Meeting Virtual-07 2024.*

2. Conferences

2.1. **Crypto 2024 Update.** *Crypto 2024* is starting in a few days, and online registration closed two days ago. The number of participants is slightly below 2023, but within the budgeted prediction.

The Board's *Strategic Meeting* will be held on Sunday, and Lepoint provides practical information. The Secretary will be attending remotely, and calls for a volunteer in-person attendee to keep the minutes of the meeting.

3. Topics

3.1. **IACR School proposal.** Lepoint presents the next item. The *Schools Committee* has received a proposal for a *Spring School on Symmetric Cryptography*, to be collocated with the conference on Fast Software Encryption (FSE) in Rome next year.

The organizers expect about 40 participants, and wish to enforce a cap at 50 participants (prioritizing participants in their first year of PhD and last year of Master's studies). The Board expresses concern about this upper limit. The venue could accommodate up to 100, but the organizers wish to enforce a cap because exercise sessions

may not scale well. The Board encourages the organizers to reconsider this limit and adapt in case the demand exceeds 50 registrations.

Regardless, the Schools Committee recommends this proposal be granted the requested amount of 9,750 EUR. The Treasurer confirms that there are available funds to cover this amount. The President calls for a vote.

Decision 2 (unanimous)**.** *The Board approves the recommendation from the Schools Committee to sponsor the Spring School on Symmetric Cryptography for 9,750 EUR.*

Lepoint wants to advertise the possibility to submit IACR Schools proposals during next week's conference *Crypto 2024*, with a deadline this Fall. The Board approves the initiative.

3.2. **Selection of the second Program Chair for Asiacrypt 2026.** One of the selected candidates for Program Chair for *Asiacrypt 2026* has declined the offer. Naofumi Homma has accepted, and we need to nominate a new co-chair. Several names have been submitted. Each candidate is presented in a few words by the person who nominated them.

Decision 3. *Manoj Prabhakaran is appointed Asiacrypt 2026 Program Chair. [Prabhakaran has since accepted.]*

A second candidate is selected in case the first declines.

3.3. **Topics for the IACR strategic meeting.** The President invites Board members to submit topics to be discussed at the upcoming Strategic Meeting at *Crypto 2024*. The following topics are proposed:

- A follow-up on the matter of the conference model and scaling issue.
- The publication model, the publishing contract with Springer, and our publication policies.
- Reviewing the financial situation, in light of the new or future costs (bookkeeping, artifacts, the new journal...)

The President invites Board members to submit other ideas via email.

4. Closing Matters

The President closes the meeting officially at 15:10 UTC.