MINUTES IACR BOARD MEETING *VIRTUAL-06 2024*

19 JUNE 2024

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 21 full time attendees with the following proxies: Yang holds Schwabe's proxy, Poettering holds Hesse'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); 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); Bo-Yin Yang (Director 2022-2024); Moti Yung (Director 2021-2023, *PKC* Steering Committee);

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

Attendees (Representatives and Others). Tanja Lange (presenting a proposal for *Eurocrypt 2027*); Tal Malkin (TCC Steering Committee Representative); Kevin McCurley (Database Administrator); Stjepan Picek (presenting a proposal for *Eurocrypt 2027*); Sven Schäge (presenting a proposal for *Eurocrypt 2027*);

Absentees (Elected). Peter Schwabe (Director 2023-2025);

Absentees (Appointed). Foteini Baldimtsi (Communications Secretary 2023-2025); 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). Hilarie Orman (Archivist); Tal Rabin (Code-of-conduct Liaison); Yu Yu (Webmaster);

2. Conferences

2.1. **Proposal to host *Eurocrypt 2027* in Eindhoven.** Tanja Lange and Sven Schäge join the meeting to present a proposal to host *Eurocrypt 2027* in Eindhoven, at the academic venue TU/e, 11–15 April 2027. Relevant documents have been communicated to the Board ahead of the meeting. The President introduces the guests, then Schäge presents the proposal in a few minutes. The Board asks a few questions. One of the concerns expressed is the size of the main auditorium: it has fewer seats than the anticipated number of participants, so plenary sessions will have to be broadcast to another room. Is that reasonable? Lange explains that they have experience broadcasting across rooms. LaMacchia asks whether there is any flexibility on the dates. Lange answers that there is not: auditoriums are only available while the students are on vacation (therefore during spring break). LaMacchia notes that the projected dates for *RWC 2027* are the week before. Lange adds that other venues in Eindhoven can be considered, but they would be more expensive.

Lange and Schäge leave the meeting. The Board continues to discuss the choice of dates. LaMacchia insists on the need to carefully plan our events well in advance to avoid conflicts across our events and with the events of neighboring communities. Preneel notes that if we want future Eurocrypt installations to be hosted in academic venues to reduce costs, they will necessarily happen during spring break.

2.2. **Proposal to host *Eurocrypt 2027* in Rotterdam.** Stjepan Picek joins the meeting to present a proposal to host *Eurocrypt 2027* in Rotterdam, 23–27 May 2027. Picek explains that they originally looked into hosting the event in Amsterdam, but that was considerably more expensive. Rotterdam offers much more reasonable prices. Picek presents the proposal in a few minutes, then the Board asks questions. In response to a question, Picek explains that they planned the proposal for three tracks, but the convention center could handle a fourth track; the impact on the cost is unknown.

Picek leaves the meeting, and the Board starts comparing the two proposals. Most costs are very similar, except for the rooms and equipment (essentially free at TU/e). That is a considerable advantage for the Eindhoven proposal, but it comes at a price: no single room can host the entire audience (if we broadcast across rooms, do we expect the audience to naturally equidistribute?), and the dates are limited to spring break (much earlier than the usual dates for *Eurocrypt*, and possibly colliding with *RWC*).

Lysyanskaya asks whether one of these proposals could host another event instead. It is noted that RWC and CHES are both projected to happen in America in 2027.

3. Topics

3.1. **Resolution to replace Rose with LaMacchia as "key executive with control".** LaMacchia presents the next item in the agenda. Greg Rose, former Treasurer of the IACR, is still registered as "key executive with control" for the IACR account at Wells Fargo. To replace Rose with LaMacchia, the Board needs to vote. The exact phrasing of the resolution is provided in the document sent to the Board ahead of the meeting.

For robustness, Preneel asks whether there could be two such "key executives with control." Maybe the President or Vice-President could join the Treasurer. LaMacchia says that he does not know whether this is possible. It is worth investigating, but for today, we can at least replace Rose with the current Treasurer. The President calls for a vote.

Decision 1 (unanimous)**.** *We, the Board of Directors of the International Association for Cryptologic Research (IACR, also "Int'l Assoc for Cryptologic Research"), hereby votes to remove Gregory G. Rose as "key executive with control," from the Int'l Assoc for Cryptologic Research's relationship with Wells Fargo Bank NA and to appoint Brian LaMacchia as the new "key executive with control of the entity."*

3.2. **Selection of Program Chairs for Crypto 2026.** The President recalls that we need to select the two Program Chairs for *Crypto 2026*. Four 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. *Nadia Heninger is appointed Crypto 2026 Program Chair. [Heninger has since accepted.]*

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

Decision 3. *Mike Rosulek is appointed Crypto 2026 Program Chair. [Rosulek has since accepted.]*

4. Closing Matters

The President closes the meeting officially at 15:54 UTC.