MINUTES IACR BOARD MEETING *VIRTUAL-11 2023*

21 NOVEMBER 2023

1. Opening Matters

1.1. **Welcome, roll of attendees, identification of proxies.** At 21:04 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: Halevi holds Lepoints's proxy, Yang holds Guo's proxy, LaMacchia holds Yang'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); Masayuki Abe (Director 2021-2023); Shai Halevi (Director 2023-2025); 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). Foteini Baldimtsi (Communications Secretary 2023-2025); Britta Hale (*Crypto 2023* General Chair (2022-2023)); Julia Hesse (*Eurocrypt 2024* General Chair (2023-2024)); Bertram Poettering (Membership Secretary 2023-2025); Damien Stehlé (*Eurocrypt 2023* General Chair (2022-2023)); Fangguo Zhang (*Asiacrypt 2023* General Chair (2022-2023));

Absentees (Elected). Jian Guo (Director 2022-2024); Tancrède Lepoint (Director 2021-2023, *Crypto 2024* General Chair (2023-2024));

Absentees (Appointed). 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.** 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-10 2023.*

2. Conferences

2.1. **Update on conferences.** Yang reports on *TCC 2023*. Everything is ready, and there is an additional sponsor. Zhang reports on *Asiacrypt 2023*. Everything is ready. There are 409 registrations, exceeding expectations. LaMacchia and Preneel report that everything is on track for *RWC 2024* and for *FSE 2024*. Yung reports on *PKC 2024*. The reviewing process is moving forward, with a good number of submitted papers.

Hesse reports on *Eurocrypt 2024*. Sponsorships are coming it. They have started to look into how to lower the cost of the reception. Unfortunately, a reception at ETH will not be possible (because there is no security on campus on Sunday). The reception will happen at the originally planned venue, with a new contract allowing for lower minimum consumption.

2.2. **CHES 2025 location.** Schwabe presents to the board a question from the CHES steering committee. A proposal to hold *CHES 2025* in Kuala Lumpur was chosen. After this decision, it was pointed out that it is hard for holders of Israeli passports to get a visa to Malaysia. Should the committee revise this decision? A discussion ensues.

Asiacrypt 2007 was organised in Malaysia, and indeed obtaining a visa was complicated for Israeli citizens (they needed special approval by the government), and so was border security, even with the visa. Today, the website of Malaysia still states that *Israel citizens who wish to enter are required visa and approval from Ministry Of Home Affairs*.

It would not be the first time a conference happens in a country were the visa situation may be difficult for some nationalities; solutions can usually be found. This case may need to be analyzed further. In conclusion, the Board asks the following two questions to the steering committee and organizers:

- How many people in the CHES community would be affected?
- Is it possible at all for them to obtain a visa?

The organizers should look into the procedure to get people invited to the country.

2.3. **PKC 2025 proposal.** A proposal to hold *PKC 2025* in Røros, Norway, has just been shared with the board. There was not much time to study it, but a few short remarks were made. The proposed dates are the week following *Eurocrypt 2025* (in Madrid), is it not a problem? Then, the location is discussed. While Røros seems very pleasant, it seems hard to reach. The closest airport is in Trondheim, three to five hours away.

The President invited to Board to send further comments by email.

3. Topics

3.1. **Editor-in-Chief for the Journal of Cryptology.** The President recalls to the Board that Rijmen's term as Editor-in-Chief for the Journal of Cryptology is ending. He is interested in renewing his appointement. After a brief discussion, the President calls for a vote.

Decision 2 (unanimous)**.** *The Board renews Vincent Rijmen's appointement as Editor-in-Chief for the Journal of Cryptology.*

3.2. **Followup on the IACR statement condemning the Hamas attack.** The President presents the final item on the agenda. Two IACR members have reached out about the IACR statement condemning the Hamas attack. They regret that the statement did not explicitly mention the civilian deaths which followed in Gaza; they were only addressed in the more globally encompassing sentence "our heartfelt sympathy and support go out to [...] all those who are suffering its ongoing consequences." The President invites the Board to discuss two questions: should a follow-up statement be issued, and when should IACR issue such statements in the future?

It is noted that the statement about the attack is in line with IACR's tradition of issuing support to our members. The IACR has occasionally commented on events that directly affected our community. This is the case here, as a large number of members live in the zone of conflict or have personal ties there. One directly measurable effect has been the cancelations of *TCC 2023* registrations from affected members.

The discussion is redirected to clarifying when statements should be made in general. There are atrocities happening all over the world, and the IACR is not commenting on them all. We need to decide when an event has a significant impact on our community or our mission. General guidelines are discussed. It is noted that the IACR website may make it difficult to interpret the nature of the statements, and why the IACR is publishing them.

Action Point **1:**
Update the IACR website to clarify the nature and role of statements.

It is recalled that IACR statements are not necessarily voted by the Board: they can also be brought up and voted on by the members during the membership meetings. This has been the case for a few of the previously published statements. That procedure is slower, which may be an issue for time-sensitive situations.

The discussion shifts back to the comments received from the two members, and whether any further statement should be published about the ongoing conflict. While the Board is unanimously horrified by the civilian suffering in Gaza, the original statement (specifically its last sentence) was already meant to cover the fallout of the October 7 attack on all sides, in a rapidly evolving situation. The discussion reaches the conclusion that a further statement from IACR is not justified at this point.

4. Closing Matters

The President closes the meeting officially at 22:55 UTC.