MINUTES IACR BOARD MEETING *VIRTUAL-10 2024*

10 OCTOBER 2024

1. OPENING MATTERS

1.1. **Welcome, roll of attendees, identification of proxies.** At 14:08 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 (when absent), Poettering holds Hesse'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, *RWC* Steering Committee); 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, *CHES* Steering Committee); Moti Yung (Director 2021-2023, *PKC* Steering Committee);

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

Attendees (Representatives and Others). Masayuki Abe (*Asiacrypt* Steering Committee);

Absentees (Elected). Bo-Yin Yang (Director 2022-2024);

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); Kevin McCurley (Database Administrator); Hilarie Orman (Archivist); Tal Rabin (Code-of-conduct Liaison); Yu Yu (Webmaster);

1.2. **Minutes of previous meetings.** Minutes of the *Strategic Meeting* in Zurich have been shared by email. The vote is postponed to leave more time for proofreading.

2. TOPICS

2.1. **Policy on IACR Statements.** At the *Eurocrypt 2024 Strategic Meeting*, the matter of revisiting our policy on publishing IACR Statements was left open. On September 26, the Board has received a petition for the publication of a statement of sympathy for the victims in Lebanon in the ongoing war, and requesting the implementation of a policy for IACR Statements. Being closely related, these points are discussed together.

On the general matter of issuing IACR Statements, the following points are made.

- Informal discussions with IACR members have indicated that many are of the opinion that the Board should not comment on matters that are not directly related to the expertise of the association. Parts of the community are uncomfortable with the notion of "IACR Statements".
- Recent events have shown that the medium of IACR Statements can create problems. It is also a delicate and time-consuming task, and concern is raised that crafting public statements is not a skill for which Board members have been selected.
- Several academic institutions have recently adopted a policy on public statements. Harvard's[1] was mentioned at the previous meeting, and Brown's was published yesterday[2].
- On the other hand, it is argued that statements are a way for the IACR to express empathy and to defend shared humanistic values.

[1] https://provost.harvard.edu/sites/hwpi.harvard.edu/files/provost/files/institutional_voice_may_2024.pdf

[2] https://policy.brown.edu/policy/public-statements

- IACR Statements can be published by referendum of the community. It is noted however that the process is heavy and imposes delays.
- We may focus our efforts on other means to support our members in need. For instance, by helping with the practical issues raised by a war for conference attendance: conferences can waive cancellation fees or late registration fees for anyone impacted. This was communicated as follows at *TCC 2023*: *"If you or your research group are impacted in any way and need help, be it to cancel your registration for TCC 2023, ask for time to decide (with late registration waivers), or additional stipends in order to counter airfare increases, please contact us at tcc2023@iacr.org and we will assist you."*

The President proposes to form a working group to draft a possible policy on IACR Statements. The Board approves.

Decision 1. *A working group will be formed to draft a policy for public IACR Statements. The adoption of that policy will be subject to a future vote.*

Regarding the publication of a statement on the situation in Lebanon, the following points are made.

- The situation is summarized. It relates to the *IACR Statement On the War in Gaza*, published on October 18, 2023 after the Hamas attack in Israel. An addendum was published on May 10, 2024 to account for the tragic evolution of the situation, particularly in Gaza, insisting on IACR's support to all our members affected by the ongoing conflict. On September 26, the Board has received a petition to issue a statement of empathy for the victims in Lebanon, where the war recently expanded.
- The first solution being discussed is to publish a new addendum to the aforementioned statement.
- It is pointed out that the existing statements have always meant to include future victims of the conflict, indiscriminately, expressing sympathy and support to "*all those who are suffering its ongoing consequences*", and "*in Gaza, Israel, and elsewhere*". It is reminded that this phrasing was chosen to anticipate the evolution of the conflict, and the fact that repeated addendums would not be a viable solution.
- The issue of simultaneously discussing (a) a new statement (or addendum) and (b) a policy restricting new statements is raised. All arguments raised to add restrictions to IACR Statements apply to this particular statement.

It is raised that the Board's sentiment on the matter might be tainted by a parallel harassment situation. The question of an addendum should be treated independently, on its own merit. The President calls for a vote on the question: should the Board publish a new addendum to the *IACR Statement On the War in Gaza* (with a potential title change)? The answer "no" wins by a small majority.

Decision 2. *The Board will not publish a new addendum (with a potential title change) to the* IACR Statement On the War in Gaza*.*

The Board reiterates its sympathy and support to all of its members suffering from the conflict, everywhere, including in Lebanon. We send our sincere wishes for your safety and the safety of your loved ones, and of all innocent people affected by this violence.

2.2. **Visa Challenges for attending *Crypto* in the US.** Guo introduces the next agenda item. He was contacted by Chinese members regarding the difficulty of obtaining visas to attend *Crypto* in the US. Guo did a survey, and communicated the following conclusions by email:

- Nine papers accepted to *Crypto 2024* are authored by individuals affiliated with institutions in China.
- For each paper, at least one co-author applied for a visa well in advance.
- It was a success for only five of the nine papers, which were presented in person – all by a student author. The other four were presented by non-authors or by authors online.
- Five senior researchers applied for visas. Only one received the visa early enough to attend, one received it too late, and the rest were denied.

This issue is not new. Due to repeated visa rejections, many senior researchers have stopped applying. Authors from other countries, such as Iran, face similar challenges. Lepoint asks if publishing all attendance information much earlier would help. Guo responds that unfortunately, visa applications do not only suffer delays: they are often rejected.

Three potential solutions are mentioned, ranked by increasing complexity:

(1) **Hybrid Conference Format:** Facilitating online talks and attendance to accommodate those unable to travel.
(2) **Rotating Locations:** Hosting *Crypto* in different countries within the Americas to reduce visa-related barriers.
(3) **Mirror Event:** Organizing a simultaneous event in another country, as trialed at *FSE 2023*.

Solution (c), a mirror event, is deemed too complex to implement effectively and is excluded from further consideration.

Schwabe and Rodríguez-Henríquez report on *CHES 2024* and *RWC 2024*, both held in Canada: it did not ease the visa situation. Additionally, some US-based students were unable to attend due to visa restrictions that prohibit reentry after leaving the country. This issue led to many online talks. If moving to Canada does not solve the problem, will there be enough volunteers in Central and South America to host *Crypto* on a regular basis (maybe every second year)?

Maintaining *Crypto* in Santa Barbara has significantly simplified its organization. Given the historic tradition of holding *Crypto* in Santa Barbara, any proposed change should be submitted for membership approval.

3. Closing Matters

The President closes the meeting officially at 15:47 UTC.