

MINUTES IACR BOARD MEETING *VIRTUAL-07 2023*

5 JULY 2023

1. OPENING MATTERS

1.1. Welcome, roll of attendees, identification of proxies. At 14:05 UTC Abdalla 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: Bishop holds Lepoint's proxy, Rijmen (and later Hale) holds Preneel's proxy, Abdalla holds Hesse's proxy (when absent), Schwabe holds Rijmen's proxy (when absent), Hesse (and later Abdalla) holds Poettering'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); Masayuki Abe (Director 2021-2023); Jian Guo (Director 2022-2024); Shai Halevi (Director 2023-2025); Peter Schwabe (Director 2023-2025); Bo-Yin Yang (Director 2022-2024); Moti Yung (Director 2021-2023, *PKC* Steering Committee);

Attendees (Appointed). Britta Hale (*Crypto 2023* General Chair (2022-2023)); Julia Hesse (*Eurocrypt 2024* General Chair (2023-2024)); Vincent Rijmen (Journal of Cryptology Editor-in-Chief 2021-2023); Damien Stehlé (*Eurocrypt 2023* General Chair (2022-2023)); Fangguo Zhang (*Asiacrypt 2023* General Chair (2022-2023));

Absentees (Elected). Tancrède Lepoint (Director 2021-2023, *Crypto 2024* General Chair (2023-2024)); Anna Lysyanskaya (Director 2022-2024); Bart Preneel (Director 2023-2025, *FSE* Steering Committee, Program Chair Contact);

Absentees (Appointed). Foteini Baldimtsi (Communications Secretary 2023-2025); Bertram Poettering (Membership Secretary 2023-2025); Bimal Roy (*Asiacrypt 2024* General Chair 2023-2024);

Absentees (Representatives and Others). Tal Malkin (*TCC* Steering Committee); Mitsuru Matsui (*Asiacrypt* Steering Committee); Kevin McCurley (Database Administrator); Hilarie Orman (Archivist); Kenny Paterson (*RWC* Steering Committee); 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.

Decision 1 (unanimous). *The Board approves the Minutes of the IACR Board Meeting Virtual-06 2023.*

2. CONFERENCES

2.1. Update on conferences. Hale provides an update on *Crypto*. Forty-three student authors have applied to have their registration fees covered. More than 100 people have already registered for the event. Parking is now managed through an app. However, during testing, Hale discovered that if a phone is linked to a foreign payment system, it becomes impossible to use the app. Fortunately, a machine will still be available on-site. The board meeting has been scheduled for Sunday, starting at 10 am and likely to continue until mid-afternoon, possibly 3 pm.

Schwabe reports on *CHES*. They are working on getting the registration page online. The final budget is pending approval, and only then will the registration open. The team is also discussing minor changes to the program.

Yang reports on *TCC*. All is going well. They are waiting for the Program Committee to determine the number of accepted papers in order to fix the start and end times of each conference day.

Zhang reports that the contract for the *Asiacrypt* conference venue is currently in processing and should be finalized soon.

2.2. **Eurocrypt 2025 proposal.** Abdalla presents the *Eurocrypt 2025* proposal, which was previously sent via email. The conference would be held in Madrid in the beginning of May. No concerns have been raised regarding the proposal. Hesse confirms having reviewed it and finds it satisfactory. The proposal mentions opening a bank account, and Abdalla suggests they could use the existing French bank account without any issue (within the EU). LaMacchia points out that the French bank account was primarily used to support local events and not technically an IACR property. If the IACR decides to maintain this account, proper paperwork will be required.

It is noted that the budget presented in the proposal is somewhat conservative, leading to higher registration fees. The President calls for a vote.

Decision 2 (unanimous). *The Board approves the proposal to host Eurocrypt 2025 in Madrid.*

2.3. **TCC 2024 proposal.** Abdalla presents the *TCC 2024* proposal, which was sent by email ahead of the meeting. The conference would take place in Milano in November 2024. The handling of finances needs further discussion, and it is suggested to communicate with the organizers regarding the possibility of using the French account for ease. The proposal involves a large team, some of whom have experience in organizing events. No concerns are raised, and the President calls for a vote.

Decision 3 (unanimous). *The Board approves the proposal to host TCC 2024 in Milano.*

2.4. **Update on the Eurocrypt 2026 proposal.** The preliminary proposal to host *Eurocrypt 2026* in Rome has been updated. The President invites the board to take a look and send comments.

2.5. **Update on FSE 2024.** The *FSE 2024* proposal, which was approved in the previous meeting, has a conflict in dates with *RWC*. It is noted that, fortunately, the FSE and RWC audiences have a small intersection. It is suggested to maintain a calendar of upcoming events to avoid such issues in the future. Conferences should be given priority over a certain period. Spring is particularly packed, with multiple conferences over a short period of time. On that note, Yung proposes to start experimenting with co-location in 2025, maybe holding PKC in Madrid.

3. TOPICS

3.1. **2023 Elections.** The President recalls that there will be elections in 2023. Several board members will be leaving or up for reelection this year, and volunteers are needed to run the election. The importance of having board members from various geographical areas and experienced individuals in the matter is emphasized.

3.2. **Schedule for next appointments.** The President announces that we need to nominate and select the General Chairs for *Crypto 2025*, and the IACR 2025 Distinguished Lecture. Nominations will be done by email before the next meeting, and the vote will take place during the next meeting (August). We will later need to select a new member for the Test-of-time award committee. The Test-of-time award committee consists of one PC from each General conference, and two members selected by the board for two years each (one replacement every year).

4. CLOSING MATTERS

Abdalla closes the meeting officially at 15:23 UTC.