# MINUTES IACR BOARD MEETING *VIRTUAL-08 2023*

9 AUGUST 2023

## 1. Opening Matters

1.1. **Welcome, roll of attendees, identification of proxies.** At 5:05 am 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 Abdalla's proxy (when absent), Halevi (then Hesse) holds Abe's proxy, Hesse holds Halevi's proxy (when absent), Guo holds Lepoint's proxy, Schwabe holds Yang'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); 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). Britta Hale (*Crypto 2023* General Chair (2022-2023)); Julia Hesse (*Eurocrypt 2024* General Chair (2023-2024)); Bertram Poettering (Membership Secretary 2023-2025); Fangguo Zhang (*Asiacrypt 2023* General Chair (2022-2023));

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

*Absentees* (Elected). Masayuki Abe (Director 2021-2023); Tancrède Lepoint (Director 2021-2023, *Crypto 2024* General Chair (2023-2024)); Anna Lysyanskaya (Director 2022-2024);

*Absentees* (Appointed). Foteini Baldimtsi (Communications Secretary 2023-2025); Vincent Rijmen (Journal of Cryptology Editor-in-Chief 2021-2023); Bimal Roy (*Asiacrypt 2024* General Chair 2023-2024); Damien Stehlé (*Eurocrypt 2023* General Chair (2022-2023));

*Absentees* (Representatives and Others). 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-07 2023.*

The President calls for a vote to approve the minutes of the *Eurocrypt 2023* strategic meeting, including a modification proposed by Preneel.

**Decision 2** (unanimous)**.** *The Board approves the Minutes of the IACR Strategic Meeting at Eurocrypt 2023.*

## 2. Conferences I

2.1. **Crypto 2025 General Chair appointement.** The Board needs to appoint the *Crypto 2025* General Chair. Four candidates have been nominated, and each is presented by the board member who nominated them. The president calls for a vote.

**Decision 3.** *Francisco Rodríquez-Henríquez is appointed Crypto 2025 General Chair. [Rodríquez-Henríquez has since accepted.]*

A runner-up is then selected [in case Rodríquez-Henríquez had turned down the position].

2.2. **Distinguished Lecture at Eurocrypt 2025.** The board needs to select the person to deliver the IACR Distinguished Lecture at *Eurocrypt 2025*. Four candidates have been nominated, each is presented by the board member who nominated them.

Following discussion, the President call for a vote.

**Decision 4.** *A nominee is selected to be invited to give the Distinguished Lecture at Eurocrypt 2025.*

A second nominee is selected in case the first turns down the invitation.

2.3. **Proposal for PKC 2024.** A proposal for PKC 2024 has been sent to the board via email ahead of the meeting. The President notes that the voting on this matter will be conducted later by email, as it is not ready for immediate decision. From the proposal, PKC 2024 would take place in April 2024 in Sydney, Australia. Yung summarises a few other key points of the proposal.

The Treasurer notes that the student and regular registration fees are very similar, and a discussion ensues. The budget structure typically involves regular attendees subsidising student attendees to some extent. The discussion continues on the accuracy of the estimated attendance and the regular/student ratio, noting that the proposed date is two weeks after RWC and FSE, and two weeks before the RSA conference.

Finally, it is noted that the free venue is a very good point: it makes for a low-risk budget (low fixed costs). The availability of this venue is not yet certain, but it should be decided promptly.

## 3. Topics

3.1. **Schools proposals.** Abdalla recalls that the Schools Committee has received three proposals for schools: ASCrypto2023, Mathematical Aspects of Post-Quantum Cryptography, and Summer School on IoT Cybersecurity. The proposals, along with the Schools Committee's recommendations, were sent to board members before the meeting.

The Schools Committee recommends that the IACR financially supports the first two proposals but not the last one. The Board discusses the proposals and recommendations. A consensus arrises that the last school, while a suitable candidate for IACR support, is happening too soon. It is suggested to grant the last school the status of "Event in Cooperation with IACR".

The President proposes to inform the Schools Committee and vote on this matter later by email.

3.2. **IACR joining the Computing Research Association (CRA).** Ahead of the meeting, LaMacchia sent an email about the possibility of the IACR joining the North American Computing Research Association (CRA). LaMacchia began by summarising the content of his email. He highlighted that organisations like IEEE-CS, ACM, SIAM, and USENIX currently have a seat at the CRA.

The IACR being international, the question of CRA's influence beyond North America is raised. LaMacchia clarifies that the CRA primarily covers the USA, Canada, and Mexico, and while they may have some influence on allies, they do not hold a direct say in policy-making circles outside of North America. The IACR could explore similar opportunities in other parts of the world.

Preneel expresses support for engaging with such organisations but raises a budget-related concern: the cost would amount to approximately 4USD per member (and 10USD if counting only North American members). Other practical points are discussed: choosing an IACR representative, ensuring continued motivation to maintain the affiliation, and whether there is a minimum term commitment.

It is proposed to reach out to individuals currently holding positions within the CRA to gather more information on CRA's action and on how international associations justify the cost for members outside North America.

## 4. Conferences II

4.1. **Update on conferences.** Hale reports on *Crypto*. So far, 499 people have registered, which is on target. The conference has received good sponsorship. The documentary team has withdrawn from participation. It is suggested to monitor the usage of the shuttle service by attendees this year. 30 volunteers will assist during the event. With triple tracks, many volunteers are needed. As the event keeps growing every year, maybe UCSB can provide increased assistance in the future?

Schwabe reports on *CHES*. The program details will be available online this week. Currently, there are 381 registrations, with the early-bird registration period ending tomorrow. The conference will have a hybrid setup, with video streams and a chat for questions. The remote attendance option is not being openly advertised.

Yang reports on *TCC*. Visa information will be released by the notification time. Most attendees will likely be housed on campus, simplifying logistics.

Zhang reports on *Asiacrypt*. The contract for the conference venue has been finalized. Information about the conference hotel and travel has been updated on the website. Guo reports that the rebuttal phase has been closed, and decisions will be made soon.

LaMacchia reports on *RWC*. It is scheduled for late March in Toronto. The venue and catering have been secured, and a call for contributed talks has been issued. Sponsorship efforts are going forward.

Preneel reports on *FSE*: everything is on track.

## 5. Closing Matters

Abdalla closes the meeting officially at 6:51 am UTC.