

MINUTES IACR BOARD MEETING *VIRTUAL-06 2026*

10 JUNE 2026

1. OPENING MATTERS

1.1. Welcome, roll of attendees, identification of proxies. At 13:38 UTC the President opens the meeting and briefly goes around for an introductory round, confirming attendees and establishing who is holding proxies.

There are 23 full time attendees with the following proxies: Halevi holds Lysyanskaya's proxy, Naya-Plasencia holds Standaert's proxy, Yang holds LaMacchia's proxy. Preneel holds Naya-Plasencia's proxy (when absent), Preneel holds Rijmen's proxy.

1.1.1. *Roll of Attendees.*

Attendees (Elected). Allison Bishop (President 2026-2028); François-Xavier Standaert, (Vice President 2026-2028); Benjamin Wesolowski (Secretary 2026-2028); Jian Guo (Director 2025-2027); Anna Lysyanskaya (Director 2025-2027); María Naya-Plasencia (Director 2024-2026); Francisco Rodríguez-Henríquez (Director 2024-2026); Peter Schwabe (Director 2026-2028, *CHES* Steering Committee); Bo-Yin Yang (Director 2025-2027, *Asiacrypt* Steering Committee); Moti Yung (Director 2024-2026, *PKC* Steering Committee);

Attendees (Appointed). Man Ho Allen Au (*Asiacrypt* 2026 General Chair (2025-2026)); Andreas Hülsing (*Eurocrypt* 2027 General Chair (2026-2027)); Tetsu Iwata (*Asiacrypt* 2027 General Chair (2026-2027)); Tancrede Lepoint (IT Manager 2026-2028); Edoardo Persichetti (*Eurocrypt* 2026 General Chair (2025-2026)); Vincent Rijmen (Journal of Cryptology Editor-in-Chief 2024-2026); Mayank Varia (*Crypto* 2026 General Chair (2025-2026));

Attendees (Representatives and Others). Gregor Leander (*FSE* Steering Committee); Kevin McCurley (Database Administrator); Kay McKelly (Web & software developer);

Absentees (Elected). Brian LaMacchia (Treasurer 2026-2028, *RWC* Steering Committee); Shai Halevi (Director 2026-2028); Bart Preneel (Director 2026-2028, Program Chair Contact);

Absentees (Appointed). Foteini Baldimtsi (Communications Secretary 2023-2026); Joppe W. Bos (IACR Communications in Cryptology Editor-in-Chief); Chitchanok Chuengsatiansup (Membership Secretary (2026-2028));

Absentees (Representatives and Others). Tal Malkin (*TCC* Steering Committee); Hilarie Orman (Archivist); Tal Rabin (Code-of-conduct Liaison); Yu Yu (Webmaster);

2. SCHOOL PROPOSAL

Persichetti presents to the Board a proposal received by the Schools Committee for the summer school *Graz Security Week 2026*. The Schools Committee recommends that IACR sponsor the school for the requested amount of 5,000€.

Decision 1 (unanimous). *The Board approves the recommendation to sponsor the Graz Security Week 2026 for 5,000€.*

2.1. Approving minutes from previous meeting. The President calls for a vote to approve the minutes of the meeting *Virtual-04 2026*.

Decision 2 (unanimous). *The Board approves the Minutes of the IACR Board Meetings Virtual-04 2026.*

3. UPDATE ON CONFERENCES

Varia reports on *Crypto 2026*. This year, there will be no online talks in the program. Authors who cannot attend in person will submit a video, which will be made available online. As a result, the number of talks requiring a time slot in the program remains uncertain. Of the 193 accepted papers, 155 authors reported a high likelihood of in-person presentation, 20 a high likelihood of not attending, and 13 are uncertain.

Schwabe reports on *CHES 2026*. Registrations are about to open. There are currently four affiliated events and two tutorials, with more potentially to be approved soon.

Yang report on *PKC 2027*. Originally, the submission deadline was set before the final notification for *Asiacrypt 2026*. The Program Chairs have since decided to move the deadline to after the *Asiacrypt 2026* notification date.

4. PROCESS TO SELECT A NEW EDITOR-IN-CHIEF FOR THE JOURNAL OF CRYPTOLOGY

The President introduces the next agenda item: the term of the current Editor-in-Chief for the Journal of Cryptology (Vincent Rijmen) ends in December this year, and the Board must appoint a successor. Rijmen explains that during the previous selection process, a committee was formed to propose a shortlist of candidates. This list was then presented to the Board, which selected the new Editor-in-Chief.

Bishop proposes following the same process for this appointment. Rijmen and Standaert volunteer to serve on the committee and will recruit two additional members from Asia and America.

5. PROPOSAL FOR CHES 2028

The CHES Steering Committee has received a proposal to host *CHES 2028* in Kaohsiung, Taiwan, in line with the usual America-Asia-Europe rotation. The proposal was shared with the Board by email ahead of the meeting. The proposed General co-Chairs are Matthias J. Kannwischer, Bo-Yin Yang, and Kai-Min Chung. The Steering Committee supports this proposal, and the Treasurer has sent positive feedback.

The President calls for a vote.

Decision 3 (unanimous). *The Board approves the proposal to host CHES 2028 in Kaohsiung, Taiwan.*

6. SELECTION OF PROGRAM CHAIRS FOR CRYPTO 2028

The President recalls that we need to select the two Program Chairs for *Crypto 2028*. Six 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 4. *Tancrède Lepoint is appointed Crypto 2028 Program Chair. [Lepoint has since accepted.]*

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

Decision 5. *A second Crypto 2028 Program Chair is selected [pending response].*

7. PROPOSAL FOR CRYPTO 2027 IN BOGOTÁ

In response to the Board's call, a proposal has been received to host *Crypto 2027* in Bogotá, Columbia, with Valérie Gauthier-Umaña as General Chair.

In parallel, discussions with UC Santa Barbara (UCSB) have continued, and an agreement on the evolution of costs for 2027 has been reached. Given that California will host the 2028 Olympic and Paralympic Games, 2028 could be an opportune year to explore alternative venues for Crypto.

However, it is unclear whether the Bogotá proposal could be deferred to 2028. After discussion, the Board does not reach a consensus. Bishop offers to discuss this issue directly with Gauthier-Umaña and UCSB to explore possible solutions.

8. WORKING GROUPS ON THE CHANGE OF MODEL FOR PUBLICATION AND CONFERENCES

Bishop opens the final agenda item with a discussion on the publication contract with Springer and its potential evolution in light of the proposed change of model for the General Conferences. Under the new model, a new hybrid journal would serve as the single publication pipeline for Asiacrypt, Crypto, and Eurocrypt. While it would be technically feasible to remain with Springer for this new journal, Naya-Plasencia reminds the Board that last year's survey showed overwhelming community support for in-house open-access publishing. Lepoint adds that in-house publishing would likely require hiring dedicated IT personnel.

The Board discusses the current publication contract and the various options for transitioning to a new model, with particular attention to concerns about indexing.

Regarding the proposal for a change of model, Lysyanskaya suggests clarifying how certain choices (such as the proposed list of areas) could be adjusted in the future. The goal is to ensure the community evaluates the proposal based on its main ideas, with the understanding that many details are intended to evolve over time.

As time runs out, the President proposes to schedule a dedicated meeting in the coming days to continue this discussion.

9. CLOSING MATTERS

The President closes the meeting officially at 15:41 UTC.