MINUTES IACR BOARD MEETING *VIRTUAL-01 2023*

25 JANUARY 2023

1. Opening Matters

1.1. **Welcome, roll of attendees, identification of proxies.** At 21h02 UTC Abdalla opens the meeting and briefly goes around for an introductory round, confirming attendees and establishing who is holding proxies. There are 20 full time attendees with the following proxies: Abdalla holds Stehlé's proxy (when absent), Bishop holds LaMacchia's proxy, Preneel holds Rijmen's proxy, Yang holds Guo's proxy, Hale holds Bishop's proxy (when absent).

1.1.1. *Roll of Attendees.*

Attendees (Elected). Michel Abdalla (President 2023-2025); Allison Bishop (Vice President 2023-2025); Benjamin Wesolowski (Secretary 2023-2025); Masayuki Abe (Director 2021-2023); Shai Halevi (Director 2023-2025); 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); 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));

Attendees (Representatives and Others). Kevin McCurley (Database Administrator); Tal Malkin (*TCC* Steering Committee);

Absentees (Elected). Brian LaMacchia (Treasurer 2023-2025); Jian Guo (Director 2022-2024);

Absentees (Appointed). Vincent Rijmen (Journal of Cryptology Editor-in-Chief 2021-2023);

Absentees (Representatives and Others). Hilarie Orman (Archivist); Tal Rabin (Code-of-Conduct Liaison); Yu Yu (Webmaster); Kenny Paterson (*RWC* Steering Committee); Mitsuru Matsui (*Asiacrypt* Steering Committee);

1.2. **Approve minutes from last BoD virtual 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-12 '22.*

2. Conferences

2.1. **Update on upcoming conferences.** Preneel reports on the organisation of *FSE*: being held in two locations simultaneously (Beijing, China, and Kobe, Japan) implies heavier logistics than usual. Schwabe reports that notifications for *RWC* accepted talks and student stipends have been sent. There are about 35 accepted talks. Yung reports that the *PKC* committee is at work, the reviewing phase nearing its end. Everything is on-track. Stehlé reports on the organisation of *Eurocrypt*: the venue is ready for triple tracks; the lunch place for the workshops burnt down but an alternative has been found. Hale reports on the organisation of *Crypto*: all is going well so far; they are getting ready for the possibility of triple tracks.

3. Topics

3.1. **Composition of IACR committees.** The Audit Committee, the Ethics Committee, and the Schools Committee need to be appointed new members. Halevi says that it is customary to have the vice president chair the Audit and Ethics committees. He adds that it would make sense to have the membership secretary part of the Ethics committee. Hale says she would be happy to volunteer for either committee. The President encourages more people to volunteer by email.

3.2. **IACR School proposals.** Lepoint presents to the board two proposals for IACR summer schools that have been submitted to the Schools Committee.

- A summer school on Privacy-Preserving Machine Learning, in Warsaw, Poland, proposed by Stefan Dziembowski. This would be the second edition of a school organised on the same topic in 2022 in Copenhagen, Denmark. Lepoint summarises the committee's opinion, which recommends to sponsor the school for 10,000 USD.
- A summer school on Security and Privacy, in Graz, Austria, proposed by Bettina Könighofer and Sujoy Sinha Roy. This would also be the second edition of a school. Lepoint summarises the committee's opinion, which recommends to sponsor the school for the requested amount of 5,000 USD.

As the recommended amount for the school in Warsaw is lower than the requested amount, a discussion ensues about the usual limit of 10,000 USD for school sponsorship. That limit was exceptionally bypassed the previous year to support such initiatives after COVID. Hale points out that the current inflationary trend may warrant an increase of the customary limit. It is pointed out that the limit was originally at 5,000 USD.

Decision 2 (unanimous)**.** *The Board approves the recommendation from the Schools Committee to sponsor the summer school on Privacy-Preserving Machine Learning for 10,000 USD.*

Decision 3 (unanimous)**.** *The Board approves the recommendation from the Schools Committee to sponsor the summer school on Security and Privacy for 5,000 USD.*

3.3. **Revision of the Program Chair guidelines.** A revision of the Program Chair guidelines is proposed to the Board by Lepoint, McCurley and Schwabe. The most substantial change concerns the replacement of WebSubRev by HotCRP as the mandatory platform to handle submissions and reviews. The President proposes to vote by email, to leave time to the board to review the modifications. Preneel thanks the authors for the overdue update, and a discussion follows on possible further modifications of the guidelines. It is notably suggested to emphasise the criticality of the timeline (in particular regarding the availability of accepted papers at the time of the event), and to ask input from previous program chairs. Nevertheless, it is agreed that this should be left for future work, and the President proposes to vote for the proposed version in the coming week.

3.4. **Page limit.** The President has added an additional topic to the agenda: Yang has submitted a proposition to the Board to update the rule for page limit at IACR conferences. The current limit of 30 pages includes references. This creates an unfortunate incentive to shorten the bibliography. The main motivation of the page limit is to ease the reviewer's work, and pressuring the bibliography has the opposite effect. Yang suggests to allow for unlimited references, and to bring down the page limit to 27 (i.e., 30 minus the average length of the references). The President says that there would be no problem to keep the limit of 30 instead of 27. He suggests to vote on the question during the next Board meeting.

4. Appointments

4.1. **Test-of-Time Award committee.** The president recalls that the Test-of-Time Award committee needs to be appointed a new member (as replacement for Nigel Smart whose term comes to an end). Four people have been nominated. The Board votes, and appoints a new member (who may accept or turn down the position) as well as a runner up, in case the first does not accept.

Decision 4. *Tal Rabin is appointed member of the Test-of-Time Award committee. [Rabin has since accepted.]*

4.2. **CiC Editor-in-Chief.** The President recalls that we need to select the second Editor-in-Chief for the IACR Communications in Cryptology journal. More nominations have been collected since the previous meeting, to a total of five. Each name is briefly presented by the person who nominated them (or a representative). The president calls for an approval vote for each of the possible candidates.

Decision 5. *All five nominations are approved as possible candidates for the CiC Editor-in-Chief position.*

5. Closing Matters

Abdalla closes the meeting officially at 23h00 UTC.