MINUTES IACR BOARD MEETING *VIRTUAL-11 '21*

16 NOVEMBER 2021

1. Opening Matters

1.1. **Welcome, roll of attendees, identification of proxies.** At 22h03 CEST Abdalla opens the meeting and briefly goes around for an introductory round, confirming attendees and establishing who is holding proxies. There are 22 full time attendees with Abe holding proxy for Guo, Schwabe for Yang, Preneel for Rijmen, LaMacchia for Heninger (when absent), and Standaert for Yung (when absent). These minutes are reordered to the original agenda for consistency.

1.1.1. *Roll of Attendees.*

Attendees (Elected). Michel Abdalla (President 2020-2022); Joppe Bos (Secretary 2020-2022); Shai Halevi (Vice President 2020-2022, *TCC* Steering Committee); Brian LaMacchia (Treasurer 2020-2022); Masayuki Abe (Director 2021-2023); Marc Fischlin (Director 2020-2021); Nadia Heninger (Director 2019-2021); Tancrède Lepoint (Director 2021-2023); Anna Lysyanskaya (Director 2019-2021); Bart Preneel (Director 2020-2022, *FSE* Steering Committee); Peter Schwabe (Director 2020-2022); Francois-Xavier Standaert (Director 2020-2022, *CHES* Steering Committee); Moti Yung (Director 2021-2023, *PKC* Steering Committee).

Attendees (Appointed). Foteini Baldimtsi (Communications Secretary (2019-2022)); Lejla Batina (*Eurocrypt'20/'21* General Chair (2019-2021)). Allison Bishop (*Crypto'22* General Chair (2021-2022)); Colin Boyd (*Eurocrypt'22* General Chair); Vladimir Kolesnikov (*Crypto'21* General Chair (2020-2021)); Douglas Stebila (Membership Secretary (2017-2022)).

Attendees (Representatives and Others). Kevin S. McCurley (Database Administrator); Tal Rabin (Code-of-conduct Liaison).

Absentees (Appointed). Jian Guo (*Asiacrypt'21* General Chair (2020-2021)); Vincent Rijmen (Journal of Cryptology Editor-in-Chief 2021–2023); Bo-Yin Yang (*Asiacrypt'22* General Chair (2021-2022)).

Absentees (Representatives and Others). Hilarie Orman (Archivist); 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. Abdalla calls for a vote to approve the minutes.

Decision 1 (unanimous)**.** *The Board approves the Minutes of the IACR Board Meeting Virtual-10 '21.*

1.3. **Election update.** The President starts with congratulating Lysyanskaya, Yang, and Guo who will serve as IACR Directors for three-year terms commencing January 1, 2022. He also thanks Bishop, Kolesnikov and Thomé for their contributions to the IACR and willingness to serve.

2. Conferences

2.1. **Update on upcoming conferences.** The Asiacrypt program is expected to posted on the website soon. Eurocrypt was the first hybrid conference and all went well.

3. Topics

3.1. **RSA Award feedback.** Abdalla and Yung recall the previous discussion around the CT-RSA Award. The plan is to advertise this award on the IACR webpage.

3.2. **Creation of an IACR subsidiary outside Nevada.** LaMacchia presents his proposal to address limitations of our Nevada Registration. The IACR was incorporated in the State of Nevada in 1983 and we remain a Nevada-based entity to this day. Some financial services such as discount currency conversion and money transfer service are no longer licensed to do business with Nevada-based entities. In order to make use of these financial services and discounts the Treasurer proposes to establish a single-member LLC subsidiary entity that is incorporated in Washington state.

McCurley thanks the Treasurer for his hard work to reduce the cost for the IACR. There is a question if there is an alternative to Wise for money transfer which can be used in Nevada. As far as the Treasurer is aware this is not available. Preneel asks if this setup with a subsidiary might not get us blacklisted since it might seem we are avoiding rules. LaMacchia will seek legal advise but this seems a reasonable way forward to realize what we want.

Decision 2 (unanimous)**.** *The Board agrees to proceed with the proposal by the Treasurer and create a subsidiary as described in the presentation.*

3.3. **Proposal for Program Chair Nomination Process.** Rabin and Yung present the outcome of the Committee working on the proposal for the Program Chair Nomination Process. This Committee consists of Abe, Preneel, Rabin and Yung.

Rabin summarizes the proposal and the proposed changes to the process for selecting a PC chair. The nomination of candidates should happen at least one week before the Board meeting. Next, the proposal outlines minimal criteria for a candidate to be considered as a potential PC for the three general conferences. These requirements include a minimum number of published papers in reviewed IACR conferences and journals, a minimum number of cryptography related new papers in the past years, a minimum number of years from first publication in IACR conferences and journals and a minimum number of membership of IACR program committees. The Board unanimously agrees that we can improve the selection process and that submission of candidates well before the Board Meeting is a good idea. There is a question why we want to introduce such set of minimal criteria since this does not seem to be a problem in practice. Rabin disagrees, she gives two examples of previous chairs who did not qualify these criteria. Bos asks if there were any issues with the program or conference in these situations. Rabin explains that these were good chairs but since they didn't publish sufficiently in IACR venues they shouldn't chair our conferences. Stebila explains he is not in favor of such minimal criteria since this makes the process less inclusive and excludes many types of career paths. Rabin believes these requirements are minimalistic and hardly cuts people out. Yung explains that these minimal criteria were initially higher and he was in favor to lower them.

There follows a discussion on these requirements and when in your career one should typically chair. Halevi explains he is against the principle of setting fixed requirement. Yang fully agrees with Stebila's position. Fischlin agrees that our current often ad-hoc decision making process can be improved. For him it is not clear what problem we are fixing and agrees with Stebila that this proposal seems exclusive. Heninger also agrees with Stebila: we need to get better organized but a set of minimum requirements is not the solution. Colin agrees with Halevi, a set of minimum requirements does not make sense. He is in favor of introducing anonymous voting in the Board for the candidates.

Bos proposes to follow the suggestion by Halevi to split this proposal into two parts and vote on this: the first one related to the early nomination and the second one on the minimum requirements. He also agree with Stebila. Even if the current set of minimum requirements does not exclude any previous chairs it does not automatically make this approach meaningful.

Preneel explains that he was part of this Committee and never was a big fan of these minimal criteria. However, they might serve as a selection tool. Stebila argues that one of the main outcomes of a good chair is a good scientific program. Rabin disagrees, a good program is not the only reason to appoint chairs. If someone took a different career path then you should not become a chair.

LaMacchia agrees that the current approach often feels a bit random. He wonders if we could ask the community for names? Schwabe explains that the CHES community is part industry and part academia. Industry is an intrinsic part of our community and these minimal criteria might be an insult to a large part of our community. Abe recalls that for *Asiacrypt* the Steering Committee has a strong preference for people who were part of the community.

The President concludes that it seems the Board agrees that deciding names on the spot in the Board meeting is not a good approach. We need a better nomination process. For the second part of the proposal there does not seem to be consensus. We see the community in different ways. There are a good set of metrics which does not necessarily need to become minimum criteria.

Halevi proposes to vote on the early nomination. There are concerns about the voting guidelines since they specifically allow to put names forward on the spot. LaMacchia proposes to call for nominations early while also allowing last-minute nominations.

Decision 3. *The Board intends to change the voting rules for the Program Chair nomination such that nominations are made at least one week before the Board Meeting.*

> Action Point **1: Bos, Abdalla** *(no time set)*:
> Create a new proposal for the voting rules for the Program Chair nomination.

3.4. **IT/web update.** Stebila presents an overview of the recent IT web updates. Most notably, the 14-year old power supply of the s2 server failed: we lost mail, various main web sites, conference registration and membership database and corporate documents. The hosting provider restored from backup to a temporary server: fortunately there is no unrecoverable data loss. The IT team is migrating services to different servers. McCurley has been dedicating a lot of time to our mail server. There is a high risk since the IACR heavily relies on knowledge in a limited number of volunteers.

Halevia would like to thank Stebila, McCurley and Cachin for their many hours after power supply failure. This reduced the impact significantly. He suggests that it is maybe time to hire somebody for our system administration. McCurley wonders how this would work in practice: who would hire and supervise this person on a day-to-day basis?

3.5. **Discussion about the new journal proposal (Eurocrypt feedback).** Bos provides a short update on the progress (due to time constraints of the Board Meeting). The proposal was presented at the *Eurocrypt* Membership meeting. This was generally well received with a number of questions; especially around the impact on the smaller conferences which are at the border of the IACR. Some members of the FSE community raised their concerns with the new Journal and the impact on the Transactions on Symmetric Cryptology.

Preneel mentions that the Transactions on Symmetric Cryptology failed to get indexed because of the lack of formal ethical statements and policies. He suggests the Board investigates this such we conform to these requirements. Moreover, the impact factor was not high enough to be included in Web of Science.

4. Closing Matters

Abdalla closes the meeting at 00h01 CEST.