MINUTES IACR BOARD MEETING *VIRTUAL-7 '21*

20 JULY 2021

1. Opening Matters

1.1. **Welcome, roll of attendees, identification of proxies.** At 16h02 CEST Abdalla opens the meeting and briefly goes around for an introductory round, confirming attendees and establishing who is holding proxies. There are 18 full time attendees with the following proxies: Preneel holds Rijmen's proxy and Schwabe holds Batina's proxy.

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); Nadia Heninger (Director 2019-2021); Anna Lysyanskaya (Director 2019-2021); Bart Preneel (Director 2020-2022, *FSE* Steering Committee); Peter Schwabe (Director 2020-2022);

Attendees (Appointed). Foteini Baldimtsi (Communications Secretary (2019-2022)); Allison Bishop (*Crypto'22* General Chair (2021-2022)); Colin Boyd (*Eurocrypt'22* General Chair previously *Eurocrypt'21* General Chair (2020-2022)); Jian Guo (*Asiacrypt'21* General Chair (2020-2021)); Vladimir Kolesnikov (*Crypto'21* General Chair (2020-2021)); Douglas Stebila (Membership Secretary (2017-2022)); Bo-Yin Yang (*Asiacrypt'22* General Chair (2021-2022));

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

Absentees (Elected). Marc Fischlin (Director 2020-2021); Tancrède Lepoint (Director 2021-2023); Moti Yung (Director 2021-2023, *PKC* Steering Committee); Francois-Xavier Standaert (Director 2020-2022, *CHES* Steering Committee).

Absentees (Appointed). Lejla Batina (*Eurocrypt'20/'21* General Chair (2019-2021)); Vincent Rijmen (Journal of Cryptology Editor-in-Chief 2021–2023).

Absentees (Representatives and Others). Hilarie Orman (Archivist).

1.2. **Approve minutes from last BoD virtual meeting.** The President thanks the Secretary and Stebila 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. *The Board approves the Minutes of the IACR Board Meeting Virtual-6 '21.*

2. Conferences

2.1. **Eurocrypt 2021.** Stjepan Picek provides the Board with an update on *Eurocrypt 2021*. This will be a hybrid event: it will be possible to attend physically while virtual attendance is possible as well. The accepted papers are online and the program should be finalized soon. It is planned to open registration by the end of July. The local organization is going along and with the current set of restrictions a hybrid event still seems possible. Sponsorship is mainly carried over from last year. Schwabe explains that the current forecast is that there will be five or six affiliated events running locally or in hybrid mode. Stebila asks if he can be contacted for the organization of the registration: the hybrid situation potentially makes things more complicated. The idea is that virtual attendees can participate for free while physical attendance require a registration fee.

McCurley provides an overview of the format for a hybrid conference. One of the central points is that remote speakers should have a good experience. One idea is that local speakers present through zoom and local participants watch this zoom presentation on-screen to ensure they see the same screen as the virtual attendees but with the presenter in the same room. The question is if we can we hook the room audio to the zoom audio without audio feedback or echo.

The President states that there are still a lot of unknowns for this hybrid event. There is still a risk that physical attendance is not possible at all. He asks the Board for their opinion. Halevi highlights that we should make sure

there is a single conference laptop where the presentations are pre-loaded. How are we going to handle Questions and Answers in a hybrid setting? We need to be optimistic although there might be more restrictions. It is time to take some risks to get back to a normal situation. The President believes there is an additional risk that not many people will show up physically.

2.2. **Crypto 2021 Update.** Kolesnikov recalls that the *Crypto 2021* registration opened last week. All is going according to plan. Registration is free and participants only have to pay for the IACR membership fee. Kolesnikov shared a logo with Board which he intends to put online such that people can use this themselves. Kolesnikov thanks McCurley and McKelly for all their help.

2.3. **Update on 2021 conferences.** The *CHES* 2021 conference is virtual. McCurley mentions that streaming on YouTube might be a problem since it is organized in China. Zoom should not be a problem. The *TCC* conference is still planned to be organized as a regular (physical) conference. Guo explains that the COVID situation in Singapore is up and down which brings some uncertainty for *Asiacrypt*. LaMacchia explains that for *RWC* different options have not been considered yet since this is too far in the future. The plan is to have a physical conference.

3. Appointments, committees, and policies

3.1. **Asiacrypt 2023 program co-chair appointment.** The President recalls the Board needs to select the second Program Co-Chair for *Asiacrypt 2023* who serves with Ron Steinfeld. Several excellent candidates are nominated, and after discussion a candidate is selected.

Decision 2. *Jian Guo is appointed Program Co-Chair for Asiacrypt 2023. [Guo subsequently accepted.]*

4. Topics

4.1. **Chair Selection Criteria.** Rabin and Yung have prepared a presentation which Rabin shares with the Board. They propose to the Board a more rigorous set of rules which should be used to select nominations for the role of Program Chairs by the Board. The idea is that these minimum set of rules increase the quality of the Program Chairs we choose.

Preneel recalls this has been discussed multiple times in the past by the Board. He is not in favor of any new strict rules for the nomination of Program Chairs. Focusing on scientific criteria only such as a publication record makes no sense since a chair is a management function and not all good researchers are necessarily good managers. If he could choose one criteria then this would be experience as a chair in the past (of a smaller event) but this criteria is not mentioned in the presentation. Stebila agrees that the current selection process is haphazard. However, the current proposal does not seem to solve this. One important improvement could be to collect nominations in advance (before the Board meeting).

Yang agrees with Preneel that the Program Chair is foremost a management position. He fears that this current proposal by Rabin and Yung will increase the current situation where we have a lot of theory papers in our main conferences. Abe explains from his experience with Asiacrypt that some selection criteria might be useful. However, he wonders what problem we are trying to solve since he sees no problem with the current selection procedure. Rabin refuses to comment publicly and promises to contact Abe privately. Fischlin is also against putting up too many rules. He agrees with Douglas that we should have more time to think about names and nominations before the Board meeting.

Halevi agrees that we should not limit the Board decisions by a set of rules. He agrees with Stebila that we should have more time to think about the nominations. Some simple selection criteria might be useful such as being an IACR member or being an active researcher in the field.

Lysyanskaya supports the proposal by Rabin and Yung.

The President agrees that the current nominations are sometimes very well thought through and sometimes not. We apply criteria in different ways on different occasions: sometimes previous experience is important and sometimes not. He agrees with Shai that we do not want to tie our hand with rules. We should have indeed more time for nominations. Specific rules for the number of publications disfavors people from industry which are a large part of our community. Rabin disagrees, people who chair a conference should publish actively since it is a research conference.

Bos suggests to ask the Board if we should continue to investigate this topic or not.

Decision 3. *The Board agrees to form a Committee to look into revision of the program selection procedure.*

This Committee should make a proposal and present this to the Board. The Committee members include Rabin, Yung and Preneel. Abe urges the Committee to pay special attention to the *Asiacrypt* conference since this was not mentioned in the presentation.

5. Closing Matters

Abdalla closes the meeting officially at 18h01 CEST.