MINUTES IACR BOARD MEETING *VIRTUAL-3 '20*

7 MAY 2020

1. Opening Matters

1.1. **Welcome, roll of attendees, identification of proxies.** At 23h04 CEST Abdalla opens the meeting and briefly goes around for an introductory round, confirming attendees and establishing who is holding proxies. There are 19 full time attendees. Lysyanskaya leaves at 00h32 CEST and Reyzin is holding her proxy.

1.2. **Review and approval of agenda.** The agenda is approved, with the understanding that the meeting will be held in an order slightly deviating from the agenda (as certain items have scheduling constraints). These minutes are reordered to the original agenda for consistency.

1.2.1. *Roll of Attendees.*

Attendees (Elected). Michel Abdalla (President 2020-2022); Shai Halevi (Vice President 2020-2022, *TCC* Steering Committee); Brian LaMacchia (Treasurer 2020-2022); Joppe Bos (Secretary 2020-2022); Masayuki Abe (Director 2018-2020); Marc Fischlin (Director 2020-2021); Nadia Heninger (Director 2019-2021); 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 2018-2020, *PKC* Steering Committee).

Attendees (Appointed). Foteini Baldimtsi (Communications Secretary (2019-2022)); Lejla Batina (*Eurocrypt'20* General Chair (2019-2020)); Colin Boyd (*Eurocrypt'21* General Chair (2020-2021)); Kwangjo Kim, (*Asiacrypt'20* General Chair (2019-2020)); Leo Reyzin (*Crypto'20* General Chair (2019-2020)); Douglas Stebila (Membership Secretary (2017-2020)); Vladimir Kolesnikov (*Crypto'21* General Chair (2020-2021)).

Attendees (Representatives and Others). Kevin S. McCurley (Database Administrator).

Absentees (Elected). Tancrède Lepoint (Director 2018-2020).

Absentees (Appointed). Jian Guo (*Asiacrypt'21* General Chair (2020-2021)); Kenny Paterson (Journal of Cryptology Editor-in-Chief 2017–2020, *RWC* Steering Committee);

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

2. Appointments, committees, and policies

Bos explains the role of the various lists and calls for suggestions for new names.

2.1. ***Eurocrypt* program co-chair appointment (one name).** The President recalls we need to appoint a Program Co-Chair for *Eurocrypt'22*. The other co-chair will be selected in the next Board Meeting. Several excellent candidates are nominated, and after discussion a candidate is selected.

Decision 1. *Orr Dunkelman is appointed Program Co-Chair for Eurocrypt'22. [Dunkelman subsequently accepted.]*

3. Status of conferences

3.1. ***Eurocrypt* virtual conference update.** McCurley gives a summary of the digital conferences and an overview of the status of the conferences plus the technology choices made. For *Eurocrypt* everything seems ready and for *PKC* the website is ready to switch over. Due to the short timeline, the plan is to use same technologies for the virtual *PKC* venue as for *Eurocrypt*.

The President asks if the Zoom chat is visible to all participants. McCurley confirms this. Abdalla mentions that if we intend to announce the Fellows then we need to create a webpage as soon as possible. Baldimtsi confirms she is already preparing this.

The number of registrations for *Eurocrypt* is already near 800. Currently there is a limit of 1000 participants for Zoom. We will probably not have that many people logged in at the same time. Moreover, people can always watch the live session on YouTube. There is a question if we should switch to a more expensive account when we see an increase of registrations on Sunday. The President decides to postpone this decision.

The President thanks McCurley for his great work to make this virtual event possible.

3.2. **Future virtual conferences: *PKC*, *CHES*.** As stated before *PKC* will be completely digital event. CHES is currently considering what to do.

3.3. ***CRYPTO* discussion.** As already communicated to the Board, the *Crypto* conference will not take place at UCSB. The President asks if we should consider moving the date for the conference. Heninger is against, this might result in a conflict for the dates of the *USENIX* and *SAC* conferences. LaMacchia agrees and suggests to stick with the original dates. Reyzin agrees that it makes a lot of sense to keep the original communicated dates. Currently they are checking what to do with the affiliated workshops. Should we offer the virtual infrastructure of *Crypto* to the affiliated events? McCurley warns this means potentially lots of issues since we need the Zoom account to prepare the main conference.

There is a question what to do with the distinguished lecture? The President warns against removing or postponing invited talks and the distinguished lecture since these attract a lot more people. Halevi agrees that doing these virtually makes a lot of sense otherwise it will get very complicated. Yung agrees that doing this electronically is best. However, if the distinguished lecturer prefers, this can be done in the next year. Reyzin proposes to see how things go at *Eurocrypt* and decide afterwards. Abdalla agrees to stick with the original dates and to decide later about the distinguished lecture.

3.4. ***TCC* update.** Halevi recalls that *TCC* is still planned in November in North Carolina and is co-located with *FOCS*. There are ongoing discussions wen we make the decision of we need to go virtual (or not) and the impact. The later we decide to cancel the higher the fee. Halevi expects that a decision will be made in July or August.

3.5. **Other conferences: *FSE*, *Asiacrypt*, *RWC*.** There is not much to update.

4. Topics

4.1. **Membership report.** Stebila presents the membership report which is shared beforehand in the repository. In response to an unsuccessful fuzzing attack on our payment system we added a captcha on most registration pages in March 2020.

4.2. **Issues for the virtual membership meeting.** The President foresees two potential topics: one about Zoom and one about contact tracing. We are very explicit that we do not endorse using Zoom and we propose to use the in-browser client. McCurley asks if the IACR should take a position with respect to contract tracing? Maybe our mass surveillance statement is good enough.

4.3. **IACR online seminars.** The President informs the Board that Farshim and Albrecht suggested the idea of having online IACR seminars. The idea is that these take place once a month. Yung likes this idea but we are currently operating in panic mode to get the conferences running. The President agrees and just wanted to inform the Board and we should keep this in the back of our minds. Heninger suggests that if we have members who volunteer and there is an audience who likes this, then this is a great initiative. McCurley indicates that streaming on YouTube would be easiest and almost no work. The President moves this as an action point for the future Board meetings.

4.4. **Future virtual board meetings.** The President asks if we intensify the meeting frequency even more over the summer. Maybe we should meet twice a month? Halevi suggests to stick to once a month and switch to more if this is needed.

4.5. **Contact tracing discussion.** There is a general discussion about contract tracing. The agreement is that the IACR should not enter the discussion which approach is best. It is likely that members will bring this topic to the attention in the Membership meeting. The President asks if we need a dedicated statement around this. Heninger points to the previous remark by McCurley that our mass surveillance statement is good enough.

There is a question where this topic is exactly coming from. Is there an explicit request from our members to create such a statement? The President is not aware of such a request. Stebila highlights that it is much more compelling if this comes from the membership. If this happens then we need a robust mechanism to vote.

There is a discussion if the virtual membership meeting counts as a real membership meeting. The agreement is that this is indeed the case. If a member asks for a vote can this be done with Zoom? If we run into technical issues, the President can always decide to create a separate Helios ballot for this.

4.6. **Code of Ethics.** The President explains that it would be good to have a Code of Ethics especially with the virtual conferences. A more general policy is needed. McCurley explains that they will amend the Code of Conduct for the virtual events.

5. Closing Matters

Abdalla closes the meeting at 1h23 CEST.