MINUTES IACR BOARD MEETING *VIRTUAL-1 '18*

12 MARCH 2018

1. Opening Matters

1.1. **Welcome, roll of attendees, identification of proxies.** At 3PM CET Cachin opens the virtual meeting over Zoom videoconference and he briefly goes around confirming attendees.

1.2. **Review and approval of agenda.** The agenda is approved and no items are added to the agenda.

1.2.1. *Roll of Attendees.* There are 21 attendees. Preneel joins at 4:09PM CET and Dunkelman leaves at 4:39PM CET and LaMacchia is holding his proxy.

Attendees (Elected). Christian Cachin (President 2017-2019); Greg Rose (Vice President 2017-2019); Brian LaMacchia (Treasurer 2017-2019); Joppe Bos (Secretary 2017-2019); Michel Abdalla (Director 2016-2018); Masayuki Abe (Director 2018-2020); Shai Halevi (Director 2017-2019, *TCC* Steering Committee); Tancrède Lepoint (Director 2018-2020); Anna Lysyanskaya (Director 2016-2018); Bart Preneel (Director 2017-2019, *FSE* Steering Committee); Phillip Rogaway (Director 2016-2018); Francois-Xavier Standaert (Director 2017-2019, *CHES* Steering Committee); Moti Yung (Director 2015-2017, *PKC* Steering Committee).

Attendees (Appointed). Orr Dunkelman (*Eurocrypt'18* General Chair 2017-2018); Marc Fischlin (*Eurocrypt'19* General Chair 2018-2019); Josef Pieprzyk (*Asiacrypt'18* General Chair 2017-2018); Tal Rabin (*Crypto'18* General Chair 2017-2018); Mike Rosulek (Communications Secretary); Douglas Stebila (Membership Secretary 2017-2020); Muthu Venkitasubramaniam, (*Crypto'19* General Chair 2018-2019).

Attendees (Representatives and Others). Xuejia Lai (*Asiacrypt* Steering Committee Representative)

Absentees (Appointed). Mitsuru Matsui (*Asiacrypt'19* General Chair 2018-2019); Kenny Paterson (Journal of Cryptology Editor-in-Chief 2017–2019, *RWC* Steering Committee);

Absentees (Representatives and Others). Kevin S. McCurley (Database Administrator); Hilarie Orman (Archivist); Yu Yu (Webmaster).

2. Committees and policies

2.1. **Ethics Committee.** Cachin recalls that Lysyanskaya has joined the Ethics Committee replacing Benaloh. The Ethics Committee 2018 consists of Anna Lysyanskaya, Phillip Rogaway, and Greg Rose (chair). Rose provides a summary of the work done by the Ethics Committee. There has been one complaint and this is currently under investigation. There is a short discussion on how to deal with inappropriate behavior on IACR venues in general and that this goes beyond the Code of Conduct which is to be discussed later.

2.2. **Fellows Committee, info.** Lysyanskaya (chair of the Fellows Selection Committee 2018) gives an update on the work of the fellows committee. The deadline to nominate fellows was December 31st 2017. The discussions are under way but it has been a slow start; this might affect the selected fellows who would like to attend Eurocrypt 2018 since the early registration deadline is soon. Dunkelman states that this problem can be resolved. Lysyanskaya asks opinions about whether it is desirable to move the submission deadline earlier in the upcoming years such that decisions can be reached in a more timely manner.

Rabin suggests that also the people who submit fellows should be notified about the decisions and that feedback on the submitted proposal is also appreciated.

2.3. **Author no-shows at conferences.** Cachin provides a summary of the informal poll among the 2017 program chairs and general chairs asking how often authors don't show up at IACR conferences, that is, papers which are not presented by their authors. This does not seem to be a wide problem; the poll showed that around half of them had one or two cases of a no-show but this was very last minute. The Board concludes no further action is needed on this topic.

Abdalla asks if we monitor specific behavior from authors and if we know if some authors do this more frequently. He inquires if we have a policy for this. Cachin reminds the Board that the IACR's conference CFPs state that either "the authors must present" or "the work must be presented." Abdalla suggests that a video-recording

is a good alternative in some scenarios. Venkitasubramaniam suggests that video-recording is a good option but live-streaming is to be preferred since this allows for asking questions. Cachin observes that this adds a burden on the local organization to make this happen.

3. Budget and financial

3.1. **IACR Budget 2018.** LaMacchia presents the IACR budget and financial status. He discusses the FY2017 financial highlights including the profit and loss for 2017 and balance sheet for 2017 as well as the FY18 proposed budget. Transferring funds to India is a continuing problem and various solutions are investigated. Most IACR venues managed to almost break-even with the exception of *CHES* and *Asiacrypt* which made a profit. The USD 40k profit by *Asiacrypt* is due to more people attending the conference than expected. The current budget for IACR schools is USD 25k.

Stebila asks about the uncategorized credit card receipts on the profit and loss statement. LaMacchia explains that these will be categorized after the financial closure of an event. Fischlin asks about the recommendation for IACR events, do we aim for a slight loss, profit or break-even? LaMacchia highlights that we aim for break-even for our events. Abdalla asks what the current credit card transaction fee is and the treasurer explains that the average is 2.45 percent.

Decision 1 (2018/03/12)**.** *The Board approves the FY18 proposed budget.*

3.2. **Schools funding 1H2018.** Abdalla presents the three IACR school proposals and the recommendation by the IACR Schools committee to sponsor each of the three schools for USD 5k. Yung asks if we can vote on the proposal to keep unnecessary discussions to a minimum, however, Dunkelman is not sure about the blockchain school and wonders if this is something we need to focus on. The chair of the Schools Committee explain that this indeed seems like a rushed submission but that this is still an important topic. Moreover, this is a resubmission and this proposal is open for everyone to attend so the committee recommends to fund this proposal.

Rogaway points out that we are a financial healthy organization and that we are stingy with our funds. Lepoint supports this proposal but wonders if we want to penalize sloppy submissions in the future.

The president suggests we vote to accept the recommendation made by the Schools Committee. Dunkelman requests if we can vote on the three schools separately. In a first round of voting, the Board decides to vote on all proposals together.

Decision 2 (2018/03/12)**.** *The Board decides to follow the recommendation by the Schools Committee and to fund all three school proposals for USD 5k each.*

The president explains that he considers the USD 5k a minimum in order to call the event an IACR School, maybe we should increase the funding per school for upcoming events. The treasurer explains that we could decide mid-year (if the Board approves) to increase the budget for schools. Abdalla states that the Schools Committee would like to know such plans in advance such that they can plan for this.

3.3. **Policy for affiliated events.** Cachin explains that the current guidelines for organizing a conference and how to budget them does not contain any specific options for affiliated events. Should we amend the default spreadsheet used for this? He asks if we need to have a default way to handle student registration for these events, if IACR members should get a discount and if people registering for these affiliated event should become IACR members.

Abdalla recalls that for *Eurocrypt* 2017 the people registering for the joint event did not automatically become IACR members. Rabin explains that the goal of the affiliated workshops in case of *Crypto* 2018 is to attract a different audience, the budget planning could be done without such membership fees and then one hopes they attend *Crypto* 2018. In case of attending an affiliated event, the registration fee of *Crypto* is lower and students can use sponsorship money. Cachin would like to have a uniform way to handle the situation with affiliated events. Rabin suggest we discuss this at a later time when we have more experience and data available. Dunkelman explains that for *Eurocrypt* 2018 the affiliated events are risk-free since the fixed costs are taken care of by the organizers of these events. Halevi supports the suggestion to discuss this at a later point in time after we have received more feedback. He wonders if we view these affiliated events as IACR events. Cachin explains that this was not mandated in the past.

The conclusion is to get more experience, collect feedback and discuss a common policy in the Board again at a later point in time.

4. Topics

4.1. **Code of Conduct for IACR-sponsored conferences.** The Ethics Committee has made a proposal for the code of conduct for IACR sponsored conferences. Rose recalls that the current proposal is in the svn and has been mailed around in advance of this virtual Board meeting. Cachin thanks the Ethics Committee for their work, such a code of conduct is needed and should be part of the general-chair guidelines.

Rogaway recalls the e-mail discussion on this topic and agrees that serious accidents reported to a first contact person should only be forwarded to the Ethics Committee if this is wanted by the person filing the complaint. Rabin expresses that she wants to be this first person of contact outside the Ethics Committee.

Lysyanskaya explains this is the first time we construct such a code of conduct and we should consider it as a work-in-progress. Maybe provide a default text but leave the option for the general chair to deviate, this modified text should then be approved by the Ethics Committee. Halevi supports this, since flexibility and a discussion in the general chair guidelines helps. Stebila wonders if the general chairs understand all the subtleties involved and if they are qualified to make such adjustments to the code of conduct. Venkitasubramaniam states that uniformity across the IACR on this topic is to be preferred. Lepoint suggests to invite an expert on this topic to give a presentation in the conference program, maybe this could be done during the membership meeting.

The president thanks for the discussion and feedback.

Decision 3 (2018/03/12)**.** *The Board decides to continue the work on the code of conduct and use the current draft text as a basis. The final text will be added to the general chair guidelines. This activity will be continued by Bos, Halevi, Lepoint, Rabin, and Rose in collaboration with the Ethics Committee.*

The exact text and if this code of conduct should be mandatory or not is to be discussed at a next Board meeting.

Rabin reiterates that there should be an independent contact person to address harassment issues. This person should decide what to do next, this might not be to contact the Ethics Committee immediately. The president points out that the general chair should be such a first contact person. Rabin disagrees since most general chairs are men and this does not work for sexual harassment. Dunkelman supports this code of conduct but expresses that dictating that this first person of contact is female might be counterproductive. Why not have multiple persons of contact? Venkitasubramaniam agrees that multiple people in this role is to be preferred. Stebila does not think that the general chair should be the first person of contact since the general chair has already enough on his plate, this should be done through the Ethics Committee. Lysyanskaya wonders who will exactly handle the complaints, who can be approached when something happens. The first person of contact should be on site, this contact person can then hand over (if needed) to the Ethics Committee. The president confirms that this is what the IACR webpage suggests. Halevi suggests that people can volunteer to become such a first person of contact and then they receive a special sticker which they can put on their badge.

The president suggests we continue this discussion at the Board meeting at *Eurocrypt*.

4.2. **Policy for Test-of-time Award.** Cachin recalls the policy for the test-of-time award which has been shared before the virtual meeting. He goes through the text to remind the Board. Rogaway reminds the Board of the context; the original proposal was based on citation count and was rejected. He considers the notion of having three separate committees of five people a significant overkill.

Lysyanskaya explains that considering just the number of citations is ambiguous. She sees no other solution than that humans do this selection work. Rabin proposes to select the test-of-time award from a time period instead of a fixed year. LaMacchia agrees with Rogaway this proposal is too complex, the fellows program runs with fewer people. He wonders why we have a committee per conference and not one committee who oversees it all. Stebila agrees and has concerns how the people for these committees are selected. Cachin explain that the reasoning was to have one award per conference and hence one committee per conference. Rabin is concerned that if we have one committee this disqualifies *Asiacrypt*. Venkitasubramaniam notes that having more people brings more diversity and wonders if we should also include papers from FOCS and STOC.

The president asks how *TCC* handles this complexity for their award. Rabin explains that for *TCC* the test of time award is selected for any paper before a certain year. Halevi adds that the award committee consists of three people and is not a lot of work. Rogaway suggests to collapse the three to one committee in the current proposal. Cachin points out that this means the current text needs to be adopted if the Board agrees with this change.

Decision 4 (2018/03/12)**.** *The Board decides to continue with the Policy for the Test-of-time Award with the current text as the basis with the exception that there should only be one committee. The policy text needs to be updated by the committee.*

Lysyanskaya suggest to use a hybrid model where three of the five members are the same for the year and the program chairs rotate depending on the conference. Yung explains that this was all considered by the committee in the process. Rabin would like to have a window time period instead of the current fixed year proposal in the text. Cachin explains that a window was considered by the committee and asks the Board if the committee should look again into this.

Decision 5 (2018/03/12)**.** *The Board decides to* not consider *a windowed time period for the Policy for the Test-of-time Award.*

Standaert explains that using a time window might give the impression that some awards are better than other (if they come from the same time window). Cachin asks for volunteers to join this committee and Lysyanskaya steps forward.

4.3. **Guidelines on insurance for events and for directors/officers liability.** Cachin explain the recent discussion on the potential need for a directors and officers liability insurance. Halevi asks what this insurance exactly protects against and Rose explains the situation where directors or officers might be held liable. Lysyanskaya agrees we need such an insurance and suggest that a lawyer should review our current policy documents. Cachin asks Lysyanskaya to follow-up with a quote. LaMacchia agrees that such an insurance is a good thing to have and should be relatively cheap. Cachin suggest we follow-up on this over e-mail.

The meeting closes at 5:04PM CET.