MINUTES IACR BOARD MEETING *VIRTUAL-2 '18*

7 NOVEMBER 2018

1. OPENING MATTERS

1.1. **Welcome, roll of attendees, identification of proxies.** At 14:00 UTC 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, with the understanding that the meeting will be held in an order slightly deviating from the agenda (as certain items have scheduling constraints). A follow-up to the discussion related to the co-chair and rolling chair model is added to the agenda and Rabin requests to add an item about a blacklist which she will clarify later. These minutes are reordered to the original agenda for consistency.

1.2.1. *Roll of Attendees.* There are 21 full time attendees with Rosulek holding a proxy for Venkitasubramaniam. Preneel joined the meeting during the discussion of Section 3.1.

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); Kenny Paterson (Journal of Cryptology Editor-in-Chief 2017–2019, *RWC* Steering Committee);

Tal Rabin (*Crypto'18* General Chair 2017-2018); Mike Rosulek (Communications Secretary); Douglas Stebila (Membership Secretary 2017-2020);

Attendees (Representatives and Others). Xuejia Lai (*Asiacrypt* Steering Committee Representative) Kevin S. McCurley (Database Administrator);

Absentees (Appointed). Mitsuru Matsui (*Asiacrypt'19* General Chair 2018-2019); Josef Pieprzyk (*Asiacrypt'18* General Chair 2017-2018); Muthu Venkitasubramaniam, (*Crypto'19* General Chair 2018-2019).

Absentees (Representatives and Others). Hilarie Orman (Archivist); Marc Rotenberg (General Counsel); Yu Yu (Webmaster).

2. CONFERENCES & BUDGET

2.1. ***RWC 2020.*** Tom Ristenpart has been appointed General Chair of the *RWC 2020* Symposium, to be held in New York, USA, in January 2020. Cachin shows the proposed budget and ask for feedback and a discussion. Rabin asks if there is a maximum number of attendees of 600. LaMacchia recalls that the cap for *RWC 2019* is 700 attendees at that this is restricted by the size of the venue. Larger venues, and blocking related hotel accommodations, cost significantly more.

Decision 1 (Unanimous)**.** *The budget of the RWC 2020 Symposium is approved.*

2.2. ***RWC 2021.*** Peter Schwabe has been appointed General Chair of the *RWC 2021* Symposium, to be held in Amsterdam, The Netherlands, in January 2021. Cachin shows the proposed budget and ask for feedback and a discussion. There is a question why the budget is significantly lower compared to *CHES 2018* which was held at the same organization. It is expalined that Schwabe made a good arrangement with the venue; moreover, at *RWC* there are no dinners and only boxed lunch meals.

Decision 2 (Unanimous)**.** *The budget of the RWC 2021 Symposium is approved.*

2.3. **Tracking sponsorship.** This item has been put on the agenda by LaMacchia and Stebila. LaMacchia describes the current situation with respect to sponsoring. In the last couple of years we have seen an increase of sponsorship for the individual conferences and workshops. However, there is no consistent IACR-wide policy how to pay this to the conferences. Currently, this is done by either paying directly to the Treasurer or to the local account of the organizers. This makes the tracking of the sponsorship more difficult for the Treasurer. LaMacchia needs to know this since we need to disclose anyone who pays over USD 5k per year in our tax filing. Stebila and LaMacchia are working on incorporating a feature in the registration system which can be used to track these payments even if they are made locally.

Yung shares his experience when organizing conferences. Sometimes it might be the case that sponsorship is intended for both the IACR work as well as for related activities. This means that also the university will use part of the sponsorship money. The Treasurer sees no problem as long as this is clear from the start and tracked. LaMacchia suggests we collect such information centrally such that next General Chairs can access this information. Yung fully agrees with this. The President asks if this has the biggest impact of *CHES* and *RWC*. The Treasurer agrees but also thinks that *Crypto* will be impacted based on the number of received sponsorship last year.

Decision 3. *All received sponsorship contributions for our conferences, workshops and symposia must be tracked centrally.*

Action Point **1: LaMacchia, Stebila** *(no time set)*:
Incorporate a feature in the registration system which can be used to track sponsorship payments even if they are made locally.

Action Point **2: LaMacchia, Stebila, Bos** *(no time set)*:
Addendum to GC guidelines to add the new sponsorship policy.

Rabin raises the question how an abstained vote exactly counts. This is discussed between Rabin and the President. It is agreed that this needs to be clarified in the bylaws.

Action Point **3: Cachin** *(no time set)*:
Clarify the bylaws with respect to voting in the event of abstentions, quorum and unanimous decisions.

2.4. **Budget update.** LaMacchia presents the IACR budget and financial status. He presents and discusses the Profit & Loss statement from January through October 2018. He indicates that he would like to investigate our investment portfolio since this has been neglected in the last couple of years and asks if there are any comments or questions. Lysyanskaya asks about the mentioned income from 2017. The Treasurer explains this can be explained by transferring money back from abroad from local accounts and this includes the reimbursement from the NSF. Stebila has a question about the low investment income compared to the previous year on the draft of the Return of Organization Exempt from Income Tax statement. LaMacchia agrees this looks strange and will investigate if this is a mistake.

3. Policies

3.1. **Test-of-time Award.** Cachin recalls the effort to create a Test-of-Time award and presents the latest draft of the text which has been shared with the Board. Abdalla asks about the decision in the text to define eligibility of a paper in year X it must have been appeared in the same conference in year $X - 15$. Cachin explains that this is a proposal made by the committee.

Abe prefers that one can choose multiple papers. This is indeed mentioned in the proposal. McCurley recommends to promote this awards much more: there is no use to give an award if no-one knows about it. Dunkelman suggests to use the IACR Twitter account for this.

There is a discussion about the conflict rules: this might lead to high-profile people not joining as program chair if they have a chance of winning this award. The President explains this should not be a problem in practice if we have two co-chairs, one co-chair can then be responsible for this award. There follows a deeper discussion related to conflict of interest. Halevi shares the text that is used in the *TCC* test-of-time award and it is agreed to add this to the current draft.

Decision 4 (Unanimous). *The Board decides to adopt the updated Policy for the Test-of-time Award (see full text below).*

Test-of-Time Awards for General Conferences

A Test-of-Time Award is given yearly for each one of the three IACR General Conferences (Eurocrypt, Crypto, Asiacrypt).

Eligibility
To be eligible for the award given at year X for a particular conference, a paper must have been published in the same conference at year $X - 15$.

Papers authored or co-authored by current members of the award committee are not eligible to receive the award that year.

Criteria
The Test-of-Time Award recognizes papers that have had a lasting impact on the field.

Nomination
Nominations are not necessary, the committee will consider and choose the eligible papers as it wishes. In addition any person can nominate a paper for the award. Nominations should come with a short justification (at most two pages).

Selection
The selection is performed by a Test-of-Time Award Committee for the particular conference. The committee will implement its selection autonomously, and no further instructions are given beyond what is stated in this document.

Number of awards
Usually one paper from the period will receive the award, but in exceptional situations this can be relaxed at the discretion of the committee.

Committee
One test-of-time award committee will decide on the awards for the General Conferences. Its composition changes yearly. The committee for awards given at year X consists of five members:

- Two members appointed by the Board of Directors. The Board appoints one new member each year and each one serves for a term of two years.
- Three ex-officio members in the form of one program chair of each General Conference in year X. In case of co-chairs, the committee chair together with the co-chairs decide on one member.

Prior to appointing new members, the Board solicits recommendations from the existing test-of-time award committee and from the steering committees of IACR.

Committee chair
The appointed committee member that serves for the second part of her/his term chairs the committee for year X. She/he is responsible for organizing the selection process and announcing how nominations may be submitted.

Ceremony
The Test-of-Time award will be presented at the respective conference in a ceremony. It is not foreseen to have a corresponding technical talk or a paper in the proceedings.

Action Point **4: Cachin** *(no time set)*:
Create the Test-of-Time committee and appoint a chair and members.

3.2. **Journal-first submissions.** Halevi has proposed this item to the agenda. He explains this is a request for comments, not something the board needs to vote on. There is a "journal first" path in an initiative from the TOPLAS journal that lets you publish your work in the journal and present it at a conference. The nice thing about this arrangement is that it does not require any heavy-duty change of publication model or processes, all it needs is bilateral agreements between the journal and participating conferences, where the conferences agree to accept for presentation papers that would be accepted under this path to the Journal of Cryptology.

Paterson likes this proposal for the IACR, it will ensure a new flow of papers to the journal. However, implementing this is in practice might be challenging. The review cycles for the Journal of Cryptology are significantly longer compared to the conferences. The President asks how we should proceed: do we want to create a try-out? Paterson and Halevi agree this sounds like a good way forward.

Preneel expresses some concerns. What if a lot of submissions to the Journal of Cryptology are received? It seems our community is moving towards a hybrid model, like *FSE* and *CHES*; there is a risk that the editorial board of the Journal of Cryptology is flooded with new submissions. Halevi prefers to try and see what happens in a trial period. He fears that moving flagship conferences to a hybrid model will be a significant disruption. Standaert agrees with Preneel that the goals of the hybrid model are to reduce the review load and increase the quality of the papers. From his experience, the reviewing for the Journal of Cryptology is much more work and involves chasing reviewers. He fears that if the number of submission for the journal increases significantly a lot of editorial members will leave. Paterson agrees this is a good point and that a culture shift is welcome. Preneel is hesitant to try this new way-of-working out: it might be hard to shut down again.

Action Point **5: Paterson, Halevi** *(no time set)*:
Work out a proposal for journal-first submissions for discussion in the next Board meeting.

3.3. **Other topics.**

3.3.1. *Program chair contact.* Cachin explains that this is Rogaway's last meeting and a replacement for this program chair contact role is needed. Multiple good candidates are discussed and the President decides to collect feedback offline and organize a vote per e-mail. Cachin thanks Rogaway for his hard work.

3.3.2. *Blacklist.* Rabin explains she is worried about a blacklist she heard of for people who want to serve as program chairs. She did not know about this list and wants to know more about this. Rogaway explains there is no such blacklist and wonders where this information is coming from.

3.3.3. *Rolling co-chair model for program chairs.* There is a discussion if and how to proceed with this item after the discussion at the previous Board meeting. Bos recalls that it was decided to pursue further work towards changing the rolling co-chair model for the general conferences. So far nothing concrete can be reported.

Rogaway explains that he is still strongly against this proposal. This will have a very negative impact on especially *Asiacrypt* where it is already difficult to find to find good local program chairs. He also foresees that this pushes events like *Crypto* in the more theoretical direction since the applied cryptography communities in the USA is smaller. Cachin asks for volunteers to form a committee to come with a proposal how to proceed.

Action Point **6: Abdalla (chair), Rose, Rogaway, Rabin, Standaert, Abe, Dunkelman** *(no time set)*:
Work out a first draft proposal how and if to proceed with the rolling co-chair model.

3.3.4. *Webpage.* McCurley explains that he has been working towards a new look and feel of the IACR website. New videos are online and he is currently looking for information about the IACR from the 1980's for archival purposes. He would like to have all (self-made) software used by the IACR to be tracked and archived. The software used by the Archivist is currently missing.

Action Point **7: Cachin** *(no time set)*:
Contact the Archivist to check in any tools used.

3.3.5. *Elections.* Cachin informs about the current status of the elections. Lepoint explains that this is since October 15 and will close November 15. A reminder will be sent out and so far 379 people have voted. Rosulek explains we are on track with the number of votes compared to previous years.

3.4. **Director & officer liability insurance.** Cachin explains the current situation with respect to a director & officer liability insurance. Due to a miscommunication no further quotes have been acquired (besides the initial quote obtained by the Treasurer). The urgency is high to move forward. LaMacchia will renew the current quote and get a second one.

Decision 5 (Unanimous)**.** *The Board authorizes LaMacchia to obtain a Director & officer liability insurance for one year.*

Cachin closes the virtual meeting at 15h56 UTC.