MINUTES IACR BOARD MEETING *CRYPTO'19*

SANTA BARBARA, USA, 18 AUGUST 2019

1. Opening Matters

1.1. **Welcome, roll of attendees, identification of proxies.** At 10h05 Cachin opens the meeting and briefly goes around for an introductory round, confirming attendees and establishing who is holding proxies. There are 20 full time attendees with Reyzin holding proxy for Lysyanskaya, Stebila holding proxy for Paterson, and Lepoint holding proxy for Baldimtsi and for Halevi (during his absence).

Halevi joins the meeting at 10h35, Matsui at 11h07, Kim at 12h45 and McCurley at 15h00.

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. There was an adjournment for lunch around 12h50.

1.2.1. *Roll of Attendees.*

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 2019-2021); Masayuki Abe (Director 2018-2020); Shai Halevi (Director 2017-2019, *TCC* Steering Committee); Nadia Heninger (Director 2019-2021); Tancrède Lepoint (Director 2018-2020); Bart Preneel (Director 2017-2019, *FSE* Steering Committee); Francois-Xavier Standaert (Director 2017-2019, *CHES* Steering Committee); Moti Yung (Director 2018-2020, *PKC* Steering Committee).

Attendees (Appointed). Lejla Batina (*Eurocrypt'20* General Chair 2019-2020); Marc Fischlin (*Eurocrypt'19* General Chair 2018-2019); Kwangjo Kim, (*Asiacrypt'20* General Chair 2019-2020); Mitsuru Matsui (*Asiacrypt'19* General Chair 2018-2019, *Asiacrypt* Steering Committee); Leo Reyzin (*Crypto'20* General Chair 2019-2020); Douglas Stebila (Membership Secretary 2017-2020); Muthu Venkitasubramaniam, (*Crypto'19* General Chair 2018-2019).

Attendees (Representatives and Others). Kevin S. McCurley (Database Administrator); Hilarie Orman (Archivist); Mike Rosulek.

Absentees (Elected). Anna Lysyanskaya (Director 2019-2021).

Absentees (Appointed). Foteini Baldimtsi (Communications Secretary 2019-2022); Kenny Paterson (Journal of Cryptology Editor-in-Chief 2017–2019, *RWC* Steering Committee);

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

1.3. **Review and approve agenda.** The agenda is approved with some minor changes.

1.4. **Review of Open Action Points.** Bos briefly reviews the status of action items identified from the previous Board meeting since *Eurocrypt'19*. See a summary below.

- 2020 IACR President, Find a new JoC Editor-in-Chief
  Still open for the new President, see the new action item defined below.
- Paterson, Cachin, Halevi, Consult PCs and revise the current proposal for the journal-first track.
  This is ongoing work and this action can be closed.
- Rose, Yung, Lysyanskaya, Create statement addressing the US visa issues.
  Rose reminds the Secretary that this was defined more broadly and does not apply to the US visa's only. Nothing happened and for *Crypto'19* four to five visa's were not delivered on time which unfortunately seems normal. Heninger inquires if we can keep track of this information. Preneel suggests that this should be reported in the General Chair report. This item can be closed.
- Cachin, Contact the Archivist to check in any tools used.
  Still open, define new action item.
- Cachin, Paterson, Update the JoC website to clarify the scope of the Journal regarding surveys and Systematization of Knowledge (SoK) papers.
  The website has been updated and does explicitly mention survey papers. This action item can be closed.

- Cachin, LaMacchia, Identify suitable candidates for sponsorship coordinator and possibly more generally for bookkeeping support.
  No progress has been made, new action item is defined.
- Cachin, Preneel, Continue to talk to Springer to clarify which conferences are being considered for ISI indexing.
  This is still ongoing, new action is defined.
- Cachin, Bos, Halevi, Lepoint, Rabin, Rose, Create a description of the code-of-conduct liaison role.
  This is still open, no work has been done. New action item is defined.
- Cachin, Get feedback from our legal adviser on the current Code-of-Conduct.
  Unfortunately no response. This action item can be closed.
- Lepoint, Preneel, Modify the HotCRP software such that it integrates with the IACR back-end and perform a private dry-run.
  This is an ongoing discussion see Section 5.3.
- Bos, Update the Policy for the Ethics Committee document with the correct names and the new size of the committee.
  This is done and action can be closed.
- Bos, Rose, Look into possible changes to the General Chair guidelines and the ethics committee policy to extend the scope of the Code of Conduct.
  This is open and a new action item has been created.
- Bos, Update the Schools Committee policy to reflect the decision taken with respect to the chair.
  This is done and action can be closed.
- Bos, Update the website with the new members of the Schools Committee.
  Abdalla inform the Secretary that Lepoint will be replacing Petkova-Nikova. The website has been updated and this action item can be closed.
- Crypto'19, Test-of-Time Committee, Appoint new members to the Test-of-Time Award committee.
  This will be done today, see Section 3.5. This action item can be closed.
- Bos,Rose, Clarify what the term "full board" exactly means.
  This is on the agenda, see Section 5.1. This action item can be closed.
- President, Update the General-Chair guidelines regarding the organization of affiliated events.
  This has been done and the action item can be closed.
- Bos, Update the General Chair guidelines with workshop chair information.
  This person needs to report to the General Chair which in case of dispute decides. This should be aligned with the previous closed action item and can be closed.
- LaMacchia, Cachin, Finish the update of the conference planner regarding the budget of workshops.
  This is almost done; the action item can be closed.
- Preneel, Draft text for a workshop proposal, this needs to include the CoI. Possibly use Batina's proposal.
  This is still ongoing, a new action item is created.
- President, Check with Venkitasubramaniam for the affiliated events.
  Done and can be closed.

Action Point **1: 2020 IACR President** *(no time set)*:
Find a new JoC Editor-in-Chief

Action Point **2: Cachin** *(no time set)*:
Contact the Archivist to check in any tools used.

Action Point **3: Cachin, LaMacchia** *(no time set)*:
Identify suitable candidates for sponsorship coordinator and possibly more generally for bookkeeping support.

Action Point **4: Cachin, Preneel** *(no time set)*:
Continue to talk to Springer to clarify which conferences are being considered for ISI indexing.

Action Point **5: Cachin, Bos, Halevi, Lepoint, Rabin, Rose** *(no time set)*:
Create a description of the code-of-conduct liaison role.

Action Point **6: Bos, Rose** *(no time set)*:
Look into possible changes to the General Chair guidelines and the ethics committee policy to extend the scope of the Code of Conduct.

Action Point **7: Preneel** *(no time set)*:
Draft text for a workshop proposal, this needs to include the CoI. Possibly use Batina's proposal.

1.5. ***Crypto'19* Status.** Venkitasubramaniam gives an overview of the status of *Crypto'19*. As of this morning there are 567 registered attendees to the main *Crypto'19* event. For the affiliated events there are 181 registered participants on Saturday and 297 on Sunday; from these 25 and 31 are not attending *Crypto*, respectively.

Student stipends where given to almost all students (roughly 60) who requested this. Moreover, 39 student speaker waivers have been handed out. In total 32 percent of all registrations is by students. In total USD 161 thousand has been received in sponsorship. In one case, we needed to negotiate and sign a sponsorship contract. Yung asks if we can create a template for such agreements since this looks like a lot of work. The President explains that these companies want to work with their template as a starting point. Cachin thanks Venkitasubramaniam for his hard work and looks forward to *Crypto'19*.

2. Officer and Appointee Reports

2.1. **Treasurer (TCC 2020 account; investment policy; broker account).** LaMacchia presents the financial highlights of the year 2019 to date. The main highlights are

- Since moving to Stripe we have reduced the average fee to 2.4 percent
- The sponsorship invoicing is now centralized
- We started using TransferWise for discounted currency conversions. We are now paying approximately 0.4 percent on EUR and AUD currency conversions to and from USD (instead of 3 percent before)

The Treasurer recommends no change in membership fee. Rose informs if the use of the TransferWise require us to file FBAR forms. LaMacchia is not sure and will look into this.

Action Point **8: LaMacchia** *(no time set)*:
Check if we need to file the FBAR due to using TransferWise.

There is a healthy attendance to our conferences. One concern is the long time to transfer money to China and India but this has not been a practical problem yet. The Treasurer summarizes the conference income and expenses. The *Crypto'18* conference made a significant profit due to the increase in sponsorship. We are currently budgeting to make a small loss: conferences such as *Eurocrypt'19* still made a profit due to higher attendance than expected.

The Treasurer explains that an additional bank account is needed for the *TCC'20* conference.

Decision 1 (Unanimous)**.** *The Board of Directors of the International Association for Cryptologic Research (IACR) approves the opening of an additional checking account at 1st Security Bank of Washington for the use of the "IACR TCC Conference" and that the following IACR members are authorized to sign disbursements and provide telephone authorizations for banking information on behalf of the "IACR TCC Conference" account: Brian A. LaMacchia (Treasurer, IACR Board) and Alessandra Scafuro (General Chair, TCC 2020).*

Orman asks about the reason to open new bank accounts. The Treasurer explains that this is to reduce risk and ease operational complexity.

Rose and LaMacchia summarize their work on a proposal for an investment policy. Rose gives an overview of the policy and explains the purpose. The full text of the policy can be found in the repository and has been shared before the Board Meeting.

The President asks how much we intend to invest in short-, medium- and long-term funds since this is not specified in the proposal. LaMacchia explains that this needs to be discussed but it is expected we do not use the mid-term funds. Orman observes that we have made money on investments before but never needed nor used this; she wonders if such a policy is worth our time. LaMacchia explains that from a long-term point of view it makes sense to maximize our return on investment. Rose explains that we need to invest this money responsibly and we need to manage the risks. However, it is not too much time to manage this responsibly. Preneel observes that we should ensure that our funds are not too much USA focused since we are an international organization. Rose and LaMacchia agree and this is to be discussed. Venkitasubramaniam suggests we could create something along the lines of the CRI funds and use this to increase student sponsorship.

The President closes the discussion and the Board votes on the proposal.

Decision 2 (Unanimous)**.** *The Board of Directors of the International Association for Cryptologic Research (IACR) approve and adopt the document titled "Investment Policy and Procedures".*

Decision 3 (Unanimous)**.** *The Board of Directors of the International Association for Cryptologic Research (IACR), authorize the Treasurer to establish and maintain brokerage trading accounts for the IACR at Fidelity Investments to be managed in accordance with the IACR's Investment Policy and Procedures.*

2.2. **JoC Editor in Chief.** Paterson shared his written report before the Board meeting over e-mail and this can also be found in the repository. He took over as Editor-in-Chief on January 1st 2017. The original 3-year term of appointment will end in December 2019 and Paterson has agreed to serve an extra year to December 2020. Working with the President and Matt Franklin (former EiC), Paterson has reduced the number of outstanding pre-electronic submissions from a starting figure of about 60 to 3. The President thanks Paterson for all his work, everything is in good shape and this is really appreciated by the Board.

2.3. **Program chair contact.** Preneel summarizes the reports from the program chairs. Individual reports have been shared before the meeting by e-mail and can be found as well in the repository. From the *Crypto* Program Chair report the two main issues are about funding related to Program Chairs and the Program Committee members and also the usage of the HotCRP reviewing software. Both will be discussed at this Board meeting: see Section 6.1 and Section 5.3, respectively.

2.4. **Communications Secretary.** Baldimtsi joins after some technical difficulties by teleconference. The President welcomes Baldimtsi to the Board. The new Communications Secretary thanks Rosulek for all his previous work in this role. Baldimtsi plans as her first task to document all the ongoing and open tasks. There seems to be a problem with some of the e-mailing scripts, this is the first thing that needs to be resolved. Moreover, she plans to look into the multiple social media account of the IACR and how posts are shared and handled. The President agrees that such a document of tasks is a very good idea and encourages Baldimtsi to share this in the repository. The President thanks Baldimtsi again for willing to serve as the Communications Secretary.

2.5. **Membership Secretary.** Stebila presents an update on the membership composition. For the year 2019 we have 2326 members, this is a new record due to inclusion of RWC. Recent activities include minor tweaks to accommodate specific conference requirements in the registration system as well as added financial summary for end-of-conference reporting to Treasurer. The Board thanks Stebila for his great job and all the new features which are now present.

3. Program Chair and other appointments

3.1. **Program and General Chair List Maintenance.** Bos explains the role of the various lists and calls for suggestions for new names.

3.2. **Eurocrypt '21-'22 Program Co-Chair appointment.** Anne Canteaut is already appointed Program Chair (rolling co-chair for *Eurocrypt'20* and *Eurocrypt'21*). Per the new decision taken by the Board (see Section 5.2) a new parallel co-chair is selected instead of a rolling co-chair. Several excellent candidates are nominated, and after discussion a candidate is selected.

Decision 4. *Francois-Xavier Standaert is appointed Program Co-Chair for Eurocrypt '21. [Upon returning to the room Standaert accepted.]*

3.3. **Crypto '21 General Chair appointment.** Several excellent candidates are nominated and after discussion two candidates are selected; both candidates subsequently declined.

3.4. **Distinguished Lecturer '21 (to be held at Asiacrypt '21).** The distinguished lecture is held annually, on invitation by the Board. Its location cycles between the three IACR general conferences. Several excellent candidates are nominated, and after discussion a candidate is selected.

Decision 5. *Andrew Yao is invited to deliver the Distinguished Lecture at Asiacrypt'21. [Yao subsequently accepted.]*

3.5. **Test-of-Time Award Committee.** The Presidents recalls how the Test-of-Time award is selected for the General Conferences. An award will be given at conference Y in year X to honor a paper published in conference Y in year $X - 15$ which has had a lasting impact on the field.

The selection committee in any year includes two members appointed by the Board of Directors, and three program chairs of the current year's IACR general conferences as ex-officio members. The two appointed members by the Board of Directors are Dan Boneh (chair) and Tatsuaki Okamoto. Okamoto will be the new chair of the committee and a new appointed member needs to be selected. Several excellent candidates are nominated, and after discussion a candidate are selected.

Decision 6. *Ueli Maurer is appointed as a member of the Test-of-time Committee for 2020-2021. [Maurer subsequently accepted.]*

4. Internal Committee appointments, reports, and decisions

4.1. **Audit Committee.** No update, a meeting is needed.

> Action Point **9: Cachin, Handschuh, Rose** *(no time set)*:
> Make sure the Audit Committee meets.

4.2. **Endowment Committee.** LaMacchia recalls that most of this has been covered in the discussion related to the Investment Policy (see Section 2.1). The President prefers to rename the Endowment Committee to Investment Committee.

> Action Point **10: Bos** *(no time set)*:
> Change the name of the Endowment Committee to Investment Committee on the website.

4.3. **Election Committee.** Cachin summarizes the status of the upcoming elections. Bos remarks that he was unable to find the nomination form on the website.

> Action Point **11: Cachin** *(no time set)*:
> Make sure the election nomination form is linked on the election website.

4.4. **Ethics Committee.** Rose gives a status update of the work performed by the Ethics Committee. There has been a case related to issues in a Program Committee which has subsequently been forwarded to the Program Chairs to deal with. Rose reminds the Board that we still need to look into possible changes to the General Chair guidelines and the ethics committee policy to extend the scope of the Code of Conduct. This action item is still active from the previous Board meeting. The President thanks Rose for his work and the provided update.

4.5. **Schools Committee.** Abdalla shared the two Schools proposals and the recommendation made by the Schools Committee before the Board meeting. Two proposals have been received: one summer school on secure multi-party computation and one proposal which is a second school on crypto innovation. The first school is asking EUR 20 thousand while the second is asking for USD 8 thousand. Abdalla observes the second proposal has a very unbalanced list of speakers (no females).

Rose wonders if we should not put a hard limit of USD 10 thousand in the Schools policy document. Preneel asks if we ever received a final report of the first edition of the school and what we should do if they refuse to select a female speaker. Abdalla confirms that such a report was not received and that he suggests to accept this proposal with a lower budget and accept conditionally on the fact that they select a female speaker.

Decision 7 (Unanimous)**.** *The Board follows the recommendation by the Schools Committee and decides to fund both school proposals for USD* 10 *thousand each. The second schools proposal is accepted conditionally: a report on the previous funded school should be received and the school should have at least one female invited speaker.*

4.6. **Code-of-conduct Liaison.** The President recalls that no update nor report has been received by the Code-of-Conduct Liaison (Rabin). Bos observes that since we created this role no report or update has been communicated to the Board: this is worrying. Cachin agrees and we need to figure out how to proceed.

> Action Point **12: Cachin** *(no time set)*:
> Contact the Code-of-Conduct Liaison to discuss how to communicate with the Board.

5. Procedures, Bylaws and Guidelines

5.1. **Board voting and bylaws.** The President recalls the motivation to clarify the bylaws with respect to board voting. This work was performed by Cachin, Stebila and Bos. The goal is to to clarify how many "yes" votes are required for a motion to pass in either the board meetings or when voting over e-mail and how absences are interpreted and effect the vote. The requested change to the bylaws will be put forward to the members of the community in a referendum.

The current task was to clarify the term "full board" in the bylaws. After a discussion the Board agrees to leave this as-is.

5.2. **Parallel co-chairs for General Conferences (AC, CR, EC).** Cachin presents a proposal made by Abdalla based on earlier work of a committee, with the aim to change from the rolling co-chair model to the parallel co-chair model. Bos reminds that this is an action from a deferred discussion from the *Eurcrypt'19* Board Meeting where there was no agreement. Orman recalls that we have been doing the rolling model for quite some time with sometimes positive and negative results. However, this does gives more flexibility. Yung prefers the senior and junior role in parallel, maybe we should not even call the junior role a co-chair. Heninger recalls that the *Usenix* conference also switched to a parallel co-chair model: the work is simply not possible alone. Serving for two years might simply be too time consuming. Venkitasubramaniam thinks the parallel co-chair model will result in better collaboration between the co-chairs. Standaert mentions that in *CHES* there are observer roles such that

people can look behind the scenes and learn how it works. Heninger mentions that other conferences use this as well, especially future chairs are included for important discussions and decisions. Reyzin states that serving for one year is much less of a burden to the people.

Preneel recalls that mentoring did not work well in the past. He proposes to use sub-chairs for specific areas. Abdalla observes that this idea can be implemented in both the rolling as well as the parallel co-chair model.

There is a question if we have sufficient skilled people for a parallel co-chair model. The President does not think this is a problem. The parallel model solves the issue with people spending time two years in a row. Orman thinks that serving is an honor and serving two years is not a problem in practice. Yung recalls that this might be a problem for students submitting papers if their supervisor is on the committee and is a co-author.

Abe thinks that in the parallel co-chair model the likelihood for a clash between the chairs is higher. The President thinks this can be avoided by choosing the chairs wisely. Stebila suggests to include the future chairs in the program committee by default and add this rule to the guidelines. Standaert asks if we also want to vote on the area (sub-)chairs; Yung wants more information before we proceed.

Batina wonders if there is any input from the *Asiacrypt* steering committee. Matsui states that this has unfortunately not yet been discussed

Lepoint wonders how to select two compatible people. What if one of the two refuses. Standaert explains that for *CHES* a list of pair of people is created to choose from.

Preneel suggest to be very careful when and how we switch. We need to prepare a careful plan when and how to switch to avoid mismatched expectations by the chairs appointed in the rolling co-chair model.

Decision 8 (Tie, decided in favor by the President)**.** *The Board decides to switch from the rolling co-char model to the parallel co-chair model for the three General Conferences.*

> Action Point **13: Cachin, Preneel** *(no time set)*:
> Communicate the switch from rolling co-chair model to the parallel co-chair model for the three General Conferences to the current Program Chairs.

5.3. **Submission software (Websubrev, HotCRP).** The President recalls the current discussion around the submission software: especially the current software Websubrev and the popular software HotCRP. The Board has a discussion about changing Websubrev to HotCRP. Halevi has no preference, he highlights that we need a maintainer for the submission software to tailor the software to our needs. This is independent of the submission software we choose. The President proposes to create a virtual machine so we can do a test run of HotCRP and see what is missing. McCurley agrees that we need to appoint a maintainer; he is willing to maintain but this is not a long-term solution. We need to find someone who can do this. Just switching submission software alone will not solve our problems. Halevi mentions we need customizations for both TCHES and ToSC in both Websubrev and HotCRP, so this is also independent.

Preneel mentions that future Chairs might have experience with HotCRP and not necessarily with Websubrev; this might be a good reason to switch. The President agrees, he has a slight bias towards HotCRP since this is used by many other conferences in the field.

Reyzin suggests we pay students who are interested in working on the required software modifications. Venkitasubramaniam disagrees, these modifications need to be performed by professionals. The President is willing to allocate funding for maintaining the submission software. He suggest to ask the creators of HotCRP if they can make the required changes to the software for us. Lepoint points out that many of the required modifications are small and easy to do. He suggests to create a fork of the software and perform these smaller tasks. The significant changes can be done in multiple steps later.

Halevi urges the Board to make a decision that we need to look for someone who works on this. Lepoint states that he might volunteer to do this; however, he needs more time to look into this.

> Action Point **14: Cachin, Lepoint, Preneel, McCurley, Halevi, Ristenpart** *(no time set)*:
> Look into the next steps needed for maintaining the submission software.

5.4. **Update of General-Chair guidelines.** The President recalls that Venkitasubramaniam and himself made edits to the General-Chair guidelines: mainly on the workshop and affiliated events text. They will ask for feedback.

> Action Point **15: Cachin** *(no time set)*:
> Consolidate all modifications made to the General Chair guidelines.

5.5. **Update of Program-Chair guidelines.** Preneel summarizes the updates to the Program-Chair guidelines. This updates text has been put in the repository. He put in an annex for TCHES and ToSC. There is still some legacy text: especially related to the published PDF version and the copy-edited version of paper. He wonders if we should delete these clauses.

Action Point **16: Preneel** *(no time set)*:
Remove the legacy clauses from the Program-Chair guidelines.

There is a discussion about the physical Program Committee meeting mentioned in the guidelines. In the budget template the default for this meeting is set to USD 5k, should this be changed? McCurley recalls that we a license for ZoomIt for virtual meetings which could be used as well.

Action Point **17: Cachin** *(no time set)*:
Change the default for the Program Committee physical meeting in the budget template to zero.

The President thanks Preneel for his work on the Program-Chair guidelines.

6. Conferences

6.1. **Support for travel and hotel.** The President outlines a lack of guidance that became apparent during *Crypto'19*, regarding sponsoring travel or hotel for program chairs. Venkitasubramaniam recalls that the General Chair guidelines states that the General Chair can decide this for program chairs and program committee members. The President explains that this is stated broader, Section 7.5 states that

> Typically free registrations can be given to the general chair(s), (student) supporters of the organizing committee, invited speakers, sponsors, and others.

Venkitasubramaniam observes that the guidelines are not clear for program chairs and we need to improve transparency. He proposes that the General Chair contacts the Program Chair and encourages the Program Chair to pay for himself but that a budget might be available. Halevi suggests to alter the text in Section 7.6 in the General Chair guidelines such that the sentence

> The General Chair may additionally decide to allocate [...] a limited amount of funding [...] for a small number of participants who might otherwise be unable to attend the conference.

It is stated that the stipends are for participants which have *difficulty to attend*. The President would like to avoid specific wording to refrain from setting new policy. He suggests to add the Program Chair to the list of people who can receive a waiver. Stebila recalls that the question from Venkitasubramaniam goes beyond just waivers and we should be explicit if we want to budget for this beforehand. Venkitasubramaniam agrees and explains that paying for travel to a conference by a Program Chair himself might be difficult since they cannot have an accepted paper and their grants might not allow this. Halevi states that it is our objective that the Program Chair comes to the conference.

Decision 9. *The Board agrees to add the program committee chair(s) explicitly to the list of people who can receive a registration waiver in Section 7.5 of the General Chair guidelines.*

Action Point **18: Venkitasubramaniam, Cachin** *(no time set)*:
Propose further changes to the General Chair guidelines with respect to waivers or coverage of expenses for discussion at the next Board Meeting.

Action Point **19: Bos** *(no time set)*:
Add the program committee chairs explicitly to the list of people who can receive a registration waiver in Section 7.5 of the General Chair guidelines.

7. Publications and Awards

7.1. **Proposal for artifact awards.** Bos explains the background of this agenda item. A detailed plan has been shared with the Board before the meeting. At *Eurocrypt'19* Ducas approached multiple people if they were interested in supporting an artifact award. An initial proposal has been made by Ducas and Albrecht and has been shared with the Board before the meeting. This proposal aims to

- encourage authors of artifact-supported articles to give open access to those artifacts (digital data, source code),
- support authors toward improving the quality of research artifacts,
- appreciate open science with a best artifact award and/or honorable mentions for contribution to open science.

Heninger asks if this is one or multiple awards. Lepoint explains that the current proposal is about one award and two notable mentions. Bos explains that the idea is not to make this mandatory but that the General Chair can decide if this such an award is useful for the conference. Halevi states he needs more information before he can make a decision. Preneel makes it clear that for *FSE* reviewers expect that publications publish their artifacts already if relevant. Reyzin thinks it will be very labor intensive to perform high-quality reviews on these artifacts; Bos explains that this would not be the main job of the reviewers but of the committee which hands out the award.

He continues that at this moment no formal proposal is on the table but we wanted to inform if this is something the Board supports. Preneel and Cachin support this and propose to move forward with an experiment but without a formal policy for the moment. Standaert recalls that also for *CHES* reviewers expect code and traces when relevant for submitted papers. These are indeed often taken into consideration and reviewed.

Decision 10. *The Board encourages experimentation including the artifact award in collaboration with the Program Chair of the event.*

8. Conference reports since last BoD Meeting

8.1. ***Eurocrypt'19.*** The *Eurocrypt'19* conference was a success. There were 549 participants to *Eurocrypt'19* and 640 participants if the affiliated events are included. The conference budgeted to loose money but due to the higher participation the conference made a significant surplus.

9. Forthcoming Conferences

9.1. ***Asiacrypt'19.*** Matsui explains that the organization for *Asiacrypt'19* is going well. The budget plan has been submitted and they are waiting for approval.

9.2. ***Eurocrypt'20.*** Batina gives a status update on *Eurocrypt'20*. Everything is going as planned. The first workshop submissions have already been received: there are 15 possible workshop slots. The Treasurer asks Batina when the initial funding is needed. Batina explains that this is only in December this year.

9.3. ***Crypto'20.*** No specific updates. Reyzin follows the work by Venkitasubramaniam closely. The Treasurer asks if a bank account is needed for *Crypto'20*. This indeed sounds like a good idea.

Decision 11 (Unanimous)**.** *The Board of Directors of the International Association for Cryptologic Research (IACR) approves the opening of an additional checking account at 1st Security Bank of Washington for the use of the "IACR Crypto Conference" and that the following IACR members are authorized to sign disbursements and provide telephone authorizations for banking information on behalf of the "IACR Crypto Conference" account: Brian A. LaMacchia (Treasurer, IACR Board) and Leo Reyzin (General Chair, Crypto 2020).*

10. Event proposals, General Chair appointments, and Steering Committee reports

10.1. **Asiacrypt Steering Committee.** No update.

10.2. **CHES Steering Committee.** Slides with some concerns have been uploaded, this was not reviewed by the *CHES* steering committee. The Board will wait for an official report by the *CHES* steering committee.

10.3. **FSE Steering Committee.** Preneel explains that *FSE'19* was a success in Paris, France. The preparations for *FSE'20* in Athens, Greece are well under way. The *FSE* steering committee has recommended a new co-editor for Transactions on Symmetric Cryptology for the year 2020-2021.

Decision 12 (Unanimous)**.** *The Board approves the proposal by the FSE Steering Committee and appoints Itai Dinur as the Editor-in-Chief (Program Chair) for the Transactions on Symmetric Cryptology for the year 2020-2021.*

10.4. **PKC Steering Committee.** Nothing to mention: *PKC'20* will take place in Edinburgh. Everything is going as planned.

10.5. **RWC Steering Committee.** No particular updates: *RWC'20* will take place in New York, USA and *RWC'21* in Amsterdam, Netherlands.

10.6. **TCC Steering Committee.** No updates.

11. Closing Matters

11.1. **Draft Agenda for Membership Meeting.** Cachin quickly recapitulates the main issues to discuss at the membership meeting, namely

- the move from rolling co-chair to the parallel co-chair model,
- the upcoming elections.

11.2. **Review of Action Points.** After a brief review of action points, Cachin closes the meeting at 18h10.