MINUTES IACR BOARD MEETING *EUROCRYPT'18*

TEL AVIV, ISRAEL, 29 APRIL 2018

1. Opening Matters

1.1. **Welcome, roll of attendees, identification of proxies.** At 9h37 Cachin opens the meeting and briefly goes around for an introductory round, confirming attendees and establishing who is holding proxies. Preneel arrives at 9h41 and Dunkelman at 9h51. Dunkelman is in and out from the meeting to take care of the local *Eurocrypt'18* organization from 17h00 on; LaMacchia is holding his 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. There was an adjournment for lunch around 13h10.

Venkitasubramaniam states that he has problems accessing the IACR subversion server where the material for the Board meeting is stored. This is quickly resolved by the president but he reminds the Board members to bring such issues to the attention in advance of the Board meeting.

1.2.1. *Roll of Attendees.* There are 14 full time attendees with Preneel holding proxy for Rose, Rabin for Abdalla, Halevi for Lysyanskaya, Dunkelman for Rogaway, Cachin for Paterson, Lepoint for Rosulek, and Abe for Matsui.

Attendees (Elected). Christian Cachin (President 2017-2019); Brian LaMacchia (Treasurer 2017-2019); Joppe Bos (Secretary 2017-2019); Masayuki Abe (Director 2018-2020); Shai Halevi (Director 2017-2019, *TCC* Steering Committee); 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). Orr Dunkelman (*Eurocrypt'18* General Chair 2017-2018); Marc Fischlin (*Eurocrypt'19* General Chair 2018-2019); Tal Rabin (*Crypto'18* General Chair 2017-2018); Douglas Stebila (Membership Secretary 2017-2020); Muthu Venkitasubramaniam, (*Crypto'19* General Chair 2018-2019).

Absentees (Elected). Michel Abdalla (Director 2016-2018); Greg Rose (Vice President 2017-2019); Phillip Rogaway (Director 2016-2018); Anna Lysyanskaya (Director 2016-2018);

Absentees (Appointed). Mitsuru Matsui (*Asiacrypt'19* General Chair 2018-2019); Kenny Paterson (Journal of Cryptology Editor-in-Chief 2017–2019, *RWC* Steering Committee); Josef Pieprzyk (*Asiacrypt'18* General Chair 2017-2018); Mike Rosulek (Communications Secretary);

Absentees (Representatives and Others). Hilarie Orman (Archivist); Xuejia Lai (*Asiacrypt* Steering Committee Representative); Kevin S. McCurley (Database Administrator); Yu Yu (Webmaster).

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

1.4. **Approve minutes from last BoD meeting and membership meeting.** The *Crypto'17* and the *Virtual-1'18* Board meeting minutes have already been approved and published online. Cachin thanks Bos for finishing the minutes in a timely manner.

1.5. **Review of Open Action Points.** Bos briefly reviews the status of action items identified from the *Crypto'17* and the *Virtual-1'18* meeting. The majority of action points are either completed or still pending with little progress to report. An overview is given below.

- {Cachin, Paterson} *Clarify the scope of the Journal regarding surveys and Systematization of Knowledge (SoK) papers.* Done. The JoC website still needs to be updated; a new action item has been created.
- {Cachin, Steering Committee Representatives} *Encourage area conferences to establish processes for video recordings.* Done. Steering committees are also encouraged to establish processes for video recordings.
- {LaMacchia, Cachin, Stebila} *Renegotiate the UCSB contract with IACR.* Done. It has been agreed with UCSB to not renew the current agreement because the tasks covered were no longer necessary by IACR, and because with CRYPTO taking place regularly at UCSB, the formal interactions between IACR and UCSB occur in the context of CRYPTO.

- {Rogaway} *Collect reports from program chairs of conferences of last 2 years and ask them about the work load in this model.* Still open, new action point has been created.
- {LaMacchia, Abdalla, Myers} *Review the GC guidelines and in particular the financial aspects.* Ongoing, new action has been created.
- {Cachin} *Coordinate the updates of GC and PC guidelines.* Ongoing, see Section 5.7 and Section 5.8.
- {Benaloh, Orman} *Clarify in the PC Guidelines the role of the Archive and how chairs can facilitate (in particular in relation to front matter).* This has been closed.
- {Preneel} *Update the PC guidelines to include the ToSC hybrid model and the relationship between Transactions on Symmetric Cryptology and Journal of Cryptology.* Ongoing and postponed until June 2018, new action item has been created.
- {Cachin, LaMacchia} *Identify suitable candidates for sponsorship coordinator.* Open. This is still needed, or, possibly, in more generality bookkeeping support. New action point has been defined. The current chairs point out that they are keeping sponsorship contact details for such a sponsorship coordinator.
- {Dunkelman} *Revise the proposed standards statement and submit it for Board approval.* No progress. Closed.
- {Cachin, Paterson} *Sort out what to do with the pre-electronic Journal of Cryptology submissions.* Ongoing. See progress reported in Section 2.2 (still 12 papers need complete processing).
- {Cachin, Paterson} *Sort out how to handle best papers for ToSC and TCHES in relationship with the JoC.* Ongoing, waiting for the steering committees to make a formal decision, new action point has been created.
- {Rosulek} *Finish the work on the news alert system.* Still open, new action point has been created.
- {Stebila} *Update the General Chair guidelines for the new registration system.* Done.
- {Lai} *Share the list used by the Asiacrypt steering Committee for potential program chair names with Bos.* Done.
- {Bos} *Update the Program and General Chair List.* Done.
- {Lysyanskaya, Rosulek} *Check and ensure all information online is up to date (fellows committee).* Done.
- {Cachin} *Kick-off the process for the Audit Committee.* Open, see Section 4.2.
- {Rose, LaMacchia} *Resume the meetings between the Endowment Committee and the Treasurer.* Closed. Last meeting was at *Crypto'17*.
- {Cachin} *Organize the vote related to the four school proposals.* Done.
- {Preneel, Cachin, Rabin, Rose, Rogaway} *Continue the effort for a CoI policy and create a new proposal using the decisions made during the BoD meeting.* Done.
- {Rabin (chair), Dunkelman, Standaert, Yung, Cachin} *Work out a new proposal for a Test of Time award.* Done.
- {Cachin} *Set up a Doodle to determine the best time to have a virtual meeting this December.* Done.
- {Dunkelman} *Put information related to carbon neutrality on the Eurocrypt'18 webpage.* Done.
- {Dunkelman, Stebila} *Align and work out any potential issues with respect to the registration for Eurocrypt'18.* Done.
- {Dunkelman} *Work out a Call for Affiliated Workshops for Eurocrypt'18.* Done.
- {Rabin, Cachin} *Work out a Call for Affiliated Workshops for Crypto'18.* Done.
- {Cachin, Preneel} *Contact Springer to clarify which conferences are being considered for ISI indexing.* Ongoing. Preneel has had contact with Springer. Issue has not been resolved. New action point created.
- {Abdalla} *Complete the financial summary and provide this to the treasurer.* Open, new action point defined.
- {Cachin} *Clarify venue status Asiacrypt'17.* Done.
- {Cachin} *Clarify status Asiacrypt'18.* Done.
- {Standaert} *Provide an update from the CHES Steering Committee.* Done.
- {Preneel} *Provide Cachin and LaMacchia with an updated budget (FSE).* Done.
- {Bos, Halevi, Lepoint, Rabin, Rose} *Continue the work on the code of conduct and use the current draft text as a basis.* Done. See Section 5.6.
- {Test-of-Time Committee} *Continue with the Policy for the Test-of-time Award with the current text as the basis.* Ongoing. See Section 5.3.

Action Point **1: Cachin, Paterson** *(no time set)*:
Update the JoC website to clarify the scope of the Journal regarding surveys and Systematization of Knowledge (SoK) papers.

Action Point **2: Rogaway** *(no time set)*:
Collect reports from program chairs of conferences of last 2 years and ask them about the work load in this model.

Action Point **3: Preneel** *(June 2018)*:
Update the PC guidelines to include the ToSC hybrid model and the relationship between Transactions on Symmetric Cryptology and Journal of Cryptology.

Action Point **4: Cachin, LaMacchia** *(no time set)*:
Identify suitable candidates for sponsorship coordinator and possibly more generally for bookkeeping support.

Action Point **5: Cachin, Paterson** *(no time set)*:
Sort out how to handle best papers for ToSC and TCHES in relationship with the JoC.

Action Point **6: Rosulek** *(no time set)*:
Finish the work on the news alert system.

Action Point **7: Cachin, Preneel** *(no time set)*:
Continue to talk to Springer to clarify which conferences are being considered for ISI indexing.

Action Point **8: Abdalla** *(no time set)*:
Complete the financial summary of *Eurocrypt'17* and provide this to the treasurer.

1.6. ***Eurocrypt'18* Status.** Dunkelman gives an overview of the status of *Eurocrypt'18*. There are 366 confirmed attendees. There has been one reported issue, with respect to the conference location, where someone with a Lebanese passport decided not to attend. Dunkelman explains that there is a special session on Blockchain on Tuesday. For this session a special morning pass has been created which one can purchase separate without requiring to become an IACR member. Dunkelman thanks Stebila for his assistance to make this happen. In total, 20 people have made use of this special morning pass. Cachin thanks Dunkelman for his hard work.

2. Officer and Appointee Reports

2.1. **Treasurer.** LaMacchia presents the financial report of the year 2017. The conferences made a bit of money, this is almost entirely due to *Asiacrypt'17* coming in well under budget. The cash flow is over USD 1.2M per year. Stebila asks if the conference income includes affiliated workshops; the treasurer explains this is indeed the case.

Transferring funds to India remains extremely difficult and unpredictable (which was required for an IACR school funding). The treasurer recommends not to change the IACR fees.

The treasurer explains that *Crypto'18*, *CHES'19*, and *RWC'19* require an US bank account for which the treasurer needs to be a signatory. He proposes to open these bank accounts at the 1st Security Bank of Washington using three separate banking resolutions and also add the general chairs of the respective conference on them. Stebila asks if there is overdraft protection and LaMacchia explains this is not the case. Moreover, there are no debit or credit cards associated to these bank accounts. Cachin thanks LaMacchia for his hard work.

Decision 1. *The Board approves the opening of three additional checking account at 1st Security Bank of Washington for the use of Crypto'18, CHES'19, and RWC'19 and that the treasurer and the respective general chair(s) are authorized to sign disbursements and provide telephone authorizations for banking information on behalf of the conference they chair.*

Action Point **9: Cachin** *(no time set)*:
Add the usage of Zoom to the PC guidelines.

2.2. **JoC Editor in Chief.** Paterson shared his written report before the meeting. Cachin summarizes the main points of the report. A special issue on TLS 1.3 is planned. There has been a significant amount of work related to the pre-electronic submissions: working with the President and Franklin (former Editor-in-Chief), the number of outstanding pre-electronic submission have reduced from a starting figure of about 60 to 12. Paterson initiated a discussion with the editorial board about term limits for board members. The consensus of the editorial board was to adopt a 5+5 model, with Associate Editors being appointed for an initial term of 5 years, renewable for a further term of 5 years by mutual consent of the Associate Editor and the Editor-in-Chief. This means Associate Editors will be leaving and new ones are appointed. Cachin thanks Paterson for his hard work.

Rabin also highlight the great work by Paterson as the Editor-in-Chief. Halevi wonders if we receive fewer submission to the JoC now we have the transactions in place. Preneel has observed that the papers from the transactions will not be encouraged to submit to JoC although we (as the Board) might like to see it differently. Standaert adds that the only submissions from CHES to JoC, as far as he is aware, are the invited best-papers.

2.3. **Program chair contact.** No program chair report has been received. It has been observed that after sending out the preliminary reviews, for conferences which have a rebuttal phase, some authors have been withdrawing papers early in order to resubmit somewhere else quicker. This is currently not seen as a problem. It is suggested that in addition to the rebuttals PC members can sometimes anonymously ask questions to authors. Venkitasubramaniam mentions that this worked really well for TCC.

2.4. **Communications Secretary.** No report has been received.

2.5. **Membership Secretary.** Stebila presents an update on the membership composition. He points out that over the last seven years membership has been relatively stable, with a slightly increased percentage of students. We have 6 senior members for 2018. The RWC Symposium held in January resulted in 529 IACR memberships for 2019 including 360 who were never a member before. Our payment processor does not support bitcoin anymore. Cachin informs if it is needed to hire additional people to do more work in this area. Stebila remarks that at the moment this is not needed. The Board thanks Stebila for his great job.

2.6. **Archivist.** No report has been received.

3. Program Chair and other appointments

3.1. **Program and General Chair List Maintenance.** Cachin quickly explains the procedure. Bos explains the role of the various lists and calls for suggestions for new names. Especially the first-time PC member list is successfully being depleted by program chairs.

3.2. **Crypto '19–'20.** Sasha Boldyreva has already been appointed as one of the co-chairs for *Crypto'19*. Several excellent candidates are nominated, and after discussion a candidate is selected.

Decision 2. *Daniele Micciancio is appointed Program Chair (rolling co-chair) for Crypto'19 and Crypto'20. [Micciancio subsequently accepted.]*

3.3. **Asiacrypt '19–'20.** Steven Galbraith has already been appointed as one of the co-chairs for *Asiacrypt'19*. Several excellent candidates are nominated, and after discussion a candidate is selected.

Decision 3. *Shiho Moriai is appointed Program Chair (rolling co-chair) for Asiacrypt'19 and Asiacrypt'20. [Moriai subsequently accepted.]*

4. Internal Committee appointments, reports, and decisions

4.1. **Fellows Committee.** Cachin explains that starting 2018, nominations for IACR fellows are now due November 15 (this is earlier than before). Lysyanskaya expresses her concern (through her proxy Halevi) that during her service time on the Fellows Committee no females have been nominated (and therefore not selected). The Board points out that members of the Fellows Committee can nominate or endorse a Fellows candidate.

4.2. **Audit Committee.** Cachin reports that an audit committee needs to be formed. LaMacchia points out that this is needed to check the treasurer by having an oversight of the financial reporting. There is a discussion if the Treasurer should be part of the audit committee and the consensus is that this is useful as long as someone else chairs this committee. The President asks if any of elected directors want to is interested to be on this committee.

Decision 4. *The audit committee will be formed and consist of Cachin, Preneel and LaMacchia.*

Action Point **10: Cachin, Preneel, LaMacchia** *(no time set)*: Find additional members for the audit committee.

4.3. **Endowment Committee.** Rabin informs what the role and tasks are of an endowment committee. LaMacchia explains that the role of the endowment committee is to manage our funds: e.g. the gift from CRI. It decides how conservative or risky we want to manage this and creates a clear policy. The President asks for volunteers for the Endowment committee.

Decision 5. *The endowment committee will be formed and consist of LaMacchia, Dunkelman, and Rose.*

Action Point **11: Cachin, LaMacchia, Dunkelman** *(no time set)*: Find additional members for the endowment committee.

4.4. **Election Committee, to be formed.** Cachin explains the role of the Election Committee and asks for volunteers.

Decision 6. *The Election Committee will be formed and consist of Abe (chair), Lepoint (returning officer), and Halevi.*

Preneel expresses his concerns with the current software used for the voting since this does not seem to be actively maintained. Maybe switching to a commercial alternative is to be preferred.

4.5. **Ethics Committee.** There is no report from the Ethics Committee. Cachin recalls that there is one reported case of harassment reported during *RWC'18*. Lysyanskaya asks (through her proxy) how we can detect wrongdoing better. LaMacchia reminds the board that the Ethics Committee has typically dealt with plagiarism and irregular submissions. These new incidents resulting from our Code of Conduct are new and we have to learn how to handle these better. Currently there is no formal policy. Cachin recalls that the Ethics Committee has the right to expel someone from the IACR. There follows a discussion that a policy is a good thing but how to handle in practice when we receive report about an incident: how should we behave and act exactly. There is no policy on how to react to such an incident resulting from the Code of Conduct. Stebila suggests we need some general guidelines. Venkitasubramaniam asks if we should get some legal advice on how to handle this. Cachin thanks the Ethics Committee and the people involved with the Code of Conduct for their difficult work.

4.6. **Schools Committee.** Currently the Schools Committee is soliciting new proposals for the next round. Rogaway proposes (through Cachin) to substantially increase the School's budget and suggests to double the annual allocation. LaMacchia asks if we should be one of the sponsors for a School or the sole funding party. Cachin explains that the budget provided per school should be used for location and student speakers; it should not be run by the IACR. Halevi wonders if increasing the amount of funding will result in more or higher quality proposals. LaMacchia does not agree that we should lose too much money on a regular basis but does agree that we can increase spending and proposes to have a look at the budget. Cachin expresses he has a somewhat opposite view; since our reserves are growing we can plan for a deficit. There is discussion around this. Halevi suggests we decide on year-to-year basis what to do with a potential surplus. LaMacchia shows a plot of our financial situation and this shows, modulo the CRI grant, that our reserves are more or less flat over the last years. Cachin would like to follow Rogaway's suggestion and increase the budget for the schools. LaMacchia objects since this means changing a single line-item on an already approved budget for this year. Dunkelman suggests we could increase the membership fees in order to increase this funding. Bos suggests to inform the School Committee that there is potentially room for an increased budget and then decide when we have received all the proposals. Yung agrees and would like to receive the best proposals. Preneel remarks that we do not simply want the schools to go to more expensive hotels or venues. Abe agrees with Bos and Yung that this is a useful suggestion to move the discussion forward. Cachin agrees and suggests the Schools Committee advocates for more budget than is currently allocated and then this should be summarized at the Board meeting at *Crypto'18*. LaMacchia agrees, we should not turn down good proposals but he highlights that we do not want to write out blank checks.

Abe reports that new members for the Schools Committee needs to be selected and approved.

> Action Point **12: Schools Committee** *(no time set)*:
> Discuss new membership for the Schools Committee for 2018.

4.7. **Legal Adviser.** As discussed previously, Marc Rotenberg (President and Executive Director of the Electronic Privacy Information Center) has volunteered to give us advice on legal matters if we officially appoint him. It is pointed out that his services will not be used to review contract of conferences. The president will be the point of contact to the Legal Adviser.

Decision 7. *The IACR will retain Marc Rotenberg as legal counselor.*

> Action Point **13: Cachin** *(no time set)*:
> Make initial contact with Rotenberg.

5. Procedures, Bylaws and Guidelines

5.1. **JoC subscriptions.** Stebila presents cost recovery for Journal of Cryptology paper copy subscriptions. The IACR currently pays Springer USD 10 for each issue of the Journal of Cryptology mailed to a member. We currently charge members USD 20 to receive 4 issues. This means that the IACR subsidizes mailing issues to each member that elects to receive paper copies. Based on JoC subscriptions as of March 14, 2018, we will be mailing at least 565 issues of JoC in 2018, at a net cost to the IACR of USD 2,825. After a brief discussion the board decided the following.

Decision 8. *As soon as feasible, the Treasurer and the Membership Secretary shall adjust paper copy subscription fees for the Journal of Cryptology for IACR members to align with the cost to the IACR of fulfilling those subscriptions, within plus or minus 10 percent at the discretion of the Treasurer to allow charging members a round number.*

5.2. **Diversity.** Following up on the Diversity agenda item that wasn't ready for the last couple of Board meetings Stebila and Rabin have made a plan how to proceed. This is presented by Stebila; the main points are outlined and the main recommendation is that the IACR should establish a task force consisting of some Board members and some non-Board members to work on these issues.

A discussion follows. Bos agrees this is a important topic and we should create such a task force. He has some questions related to the details mentioned in the text; (1) why should there be a special meet-and-greet type events for women at IACR conferences to promote networking? Many male attendees can benefit from such networking events as well. (2) Why when talking about improving diversity the emphases is especially on representation of women and people from Asia? Why not other regions (e.g. Africa or Latin America)? (3) Is the proposed local child-care information and potentially providing stipends only available for women or also for men who come with children? Rabin explains that (1) all other breaks of the conference can be considered as networking for men, (2) the plan is to start and focus on Asia and then other regions might follow and (3) this is for both men and women. Yung suggests to solicit universities to bring more undergrads to the conference. Dunkelman suggests to have diversity and inclusion events which are common in other communities such as a diversity lunch. LaMacchia fully supports this initiative and points out that there is funding room if this is required to realize this. Cachin thank Rabin and Stebila for their work and the Board agrees on the following.

Decision 9. *The Board approves the establishment of a task force to propose modifications to IACR policies, including general chair guidelines, that*

- *support women attending IACR events*
- *promote and support IACR and other events that advance diversity (defined broadly)*
- *improve diversity, especially representation of women, underrepresented populations, and people from Asia, within IACR governance.*

The task force will have an initial mandate of 2 years, and will report to the Board at each of its in-person meetings during the 2 year mandate.

The Board appoints Rabin and Stebila to form and run the task force.

5.3. **Test-of-time award.** The committee working on this only started a couple of days before this Board Meeting. The text still needs to be updated.

> Action Point **14: Test-of-Time Committee** *(no time set)*:
> 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.

Rabin (chair of the Test-of-Time Committee) suggests to do the voting on the final text per e-mail.

5.4. **Policy on free registrations.** We have discussed whether there should be a uniform policy on free registrations, for organizers, program/general chairs, helpers and others. Stebila provides an overview of the current situation split per conference and workshop. The General Chair is often part of the unpaid assistance and could therefore receive a free registration, this is marked in the planning document of the conference. For *Crypto* there have always been one free faculty and two free student registrations for UCSB. Cachin recommends that we continue handling such questions without a strict policy, but amend the relevant documents with the text as provided in the subversion system in order to be more transparent. Halevi comments that elected Board Members should never get free registration. Everyone agrees we need transparency in the conference report. Stebila argues that we need to be explicit about the situation with General Chairs since they shouldn't decide about their own financial benefit. This is made clear and the text provided by Cachin is adjusted.

Decision 10. *The Board decides to amend the General Chair Guidelines and the Conference Budget Planner with the text as discussed and stored in the subversion system.*

5.5. **Directors and Officers insurance.** LaMacchia contacted an insurance carrier to inquire about quotes on D&O liability and insurance for US events plus foreign events coverage. This latter is most likely not needed.

> Action Point **15: LaMacchia** *(no time set)*:
> Share the quotes for the Directors and Officers insurance when they are available.

Yung suggests we also add personal indemnification to the bylaws. Cachin suggests we discuss this at another Board meeting.

5.6. **Code of Conduct.** This has been discussed during *Virtual-1'18* Board Meeting. Bos, Halevi, Lepoint, Rabin, Rose worked out a new text and this has been incorporated in the General Guidelines and mailed around before the Board Meeting. This new text is discussed and studied by the board. Dunkelman objects against making this Code of Conduct text mandatory to include in the description of the event and asks for a formal vote. This vote fails. Fischlin suggests that this new text is also incorporated in the webpage template.

Cachin sees three ways how to move forward. Either existing board member takes up additional possibility, a new position as an appointed Board Member is created, or a new position as an observer or a special role is created. Halevi wonders if this should be part of the Ethics Committee. Rabin thinks it is a deterrent for people if this person is part of the Ethics Committee. Bos suggests that if there are deterrents to approach the Ethics Committee then this should be addressed. Lepoint agrees that this role should not be part of the Ethics Commitee since going to this Committee can be seen as the next step in the process.

There is a discussion around this new role which is denoted as as the *Code-of-Conduct Liaison*. LaMacchia suggests this should be a person on-site and not a global role. Yung suggests we need to have a person who has a global overview. Halevi wants both these roles. Stebila suggests that we create a board level observer role which has as a role to ensure there is a local contact point.

There are multiple votes which result in the following decision.

Decision 11. *There will be a code-of-conduct liaison role which participates as observer in the meetings of the board of directors. This role will be fulfilled by Rabin.*

Decision 12. *Amend the General Guidelines to incorporate the Code-of-Conduct.*

Action Point **16: Stebila** *(no time set)*:
Add the new Code of Conduct to the webpage template.

Action Point **17: Cachin, Bos, Halevi, Lepoint, Rabin, Rose** *(no time set)*:
Create a description of the code-of-conduct liaison role.

Action Point **18: Cachin** *(no time set)*:
Get feedback from our legal adviser on the current Code-of-Conduct.

5.7. **Update of General-Chair guidelines.** Cachin has identified multiple issues in the General-Chair guidelines due to historical reasons.

Action Point **19: Cachin, Rabin, Fischlin** *(no time set)*:
Coordinate to update the General Chair guidelines.

5.8. **Update of Program-Chair guidelines.** Cachin has identified multiple issues in the Program-Chair guidelines due to historical reasons.

Action Point **20: Cachin, Rogaway, Fischlin** *(no time set)*:
Coordinate to update the Program Chair guidelines.

6. Conferences

6.1. **Affiliated workshops at conferences.** Cachin reminds the Board that a policy for affiliated events is still needed. After a brief discussion a decision is made.

Decision 13. *Policy for IACR affiliated events is to be budget neutral and registration for these events does not require to become an IACR member.*

Action Point **21: Officers** *(no time set)*:
Update the text in the budget spreadsheet to accommodate the affiliated events.

7. Conference reports since last BoD Meeting

7.1. ***Asiacrypt'17.*** Nothing to report. The financial statement has been submitted.

7.2. ***Crypto'17.*** Nothing to report.

8. Forthcoming Conferences

8.1. ***Crypto'18.*** *Crypto'18* will be held at UCSB from August 19-23. Rabin (General Chair *Crypto'18*) informs the Board that everything is on track including sponsorship. The registration site should be up in the next couple of days and the twitter account is already working. There is some uncertainty related to some of the affiliated events; most notably the Blockchain event. The success with respect to getting more sponsors is used to help to fund more students. Rabin asks if she can use this funding to help post-docs as well. Cachin refers to the guidelines and explains this flexibility is indeed here as long as we are transparent. Rabin mentions that the stipend webpage is up and running.

8.2. ***Asiacrypt'18.*** There has been a status update from Pieprzyk for *Asiacrypt'18*. The *Asiacrypt'18* call for papers is out. Three sponsorship have been received so far. Everything is going as planned.

8.3. ***Eurocrypt'19.*** Fischlin gives a status update on *Eurocrypt'19*. Everything is going as planned. The venue has been booked and final decisions are being made related to catering. The website is up. Fischlin is strongly encouraged to have affiliated events for *Eurocrypt'19*.

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

9.1. **Asiacrypt '20 proposal and general chair appointment.** Kwangjo Kim presents his proposal for *Asiacrypt'20* in Daejeon, Korea. The plan is to have *Asiacrypt'20* from December 6 to 10. There are some questions about the local organization which are all answered by Kim. Cachin thanks Kim for this proposal.

Decision 14 (Unanimous)**.** *The proposal for Asiacrypt 2020 in Daejeon, Korea is accepted, with Kwangjo Kim as General Chair.*

9.2. **Eurocrypt '20 proposal and general chair appointment.** Batina and Picek present their proposal for *Eurocrypt'20* in Zagreb, Croatia. The first option is to host *Eurocrypt'20* from May 3 to May 7, 2020 with May 10 to May 14, 2020 as a fall-back. There are some questions who will be appointed as member of the board and this is clarified (Lejla Batina). Cachin thanks Batina and Picek for this proposal.

Decision 15 (Unanimous)**.** *The proposal for Eurocrypt 2020 in Zagreb, Croatia is accepted, with Lejla Batina and Stjepan Picek as General Chairs.*

9.3. **CHES Steering Committee.** Standaert provides a quick summary. *CHES'18* will take place in Amsterdam, the Netherlands and *CHES'19* in Atlanta, USA. It should be noted that *CHES'19* is no longer co-located with *Crypto*.

9.4. **FSE Steering Committee.** There is not much to report.

9.5. **PKC Steering Committee.** Yung recalls that *PKC'18* took place in Rio De Janeiro, Brazil and less than a 100 people attended.

9.6. **TCC Steering Committee.** Halevi recalls that *TCC'17* took place in Baltimore, USA. Half of the attendants were students.

9.7. **RWC Steering Committee.** *RWC'19* will take place in San Jose, USA. Around 700 people are expected to attend.

10. Other Matters

Cachin starts a discussion if we should have a third physical Board meeting or maybe another virtual one in order to address pending issues more efficiently. A good option for the physical meeting would be at *Asiacrypt* or *RWC*. Standaert suggests that we keep the two physical meetings and a single virtual one but have them rotating between the flagship conferences. Stebila suggests that we enable virtual attendance during the physical board meeting. Cachin sees a problem here because virtual attendents and physical ones are not at the same level. Abe remarks that the *Asiacrypt* Steering Committee already meets during *Asiacrypt* and that two meetings during one event is too much. However, it would be good if *Asiacrypt* is treated in the same way as the other flagship conferences. Preneel points out that it is not feasible and realistic to ask of people to attend an 8-hour virtual meeting; maybe they can join for a 4-hour time-slot? Cachin concludes that we should either keep two physical meetings with one or two virtual meetings or also increase the number of physical meetings with the option to join remotely. It is agreed that this should be discussed with the entire board over e-mail and that we come back to this at *Crypto'18*.

Action Point **22: Cachin** *(no time set)*:
Continue this discussion with the entire Board over e-mail related to the number of physical and virtual Board meetings.

11. Closing Matters

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

- The newly established Code-of-Conduct.
- The Code-of-Conduct liason role.
- The diversity task force.

11.2. **Review of Action Points.** After a brief review of action points, Cachin closes the meeting at 18h11.