

MINUTES IACR BOARD MEETING *EUROCRYPT'19*

DARMSTADT, GERMANY, 19 MAY 2019

1. OPENING MATTERS

1.1. **Welcome, roll of attendees, identification of proxies.** At 9h33 Cachin opens the meeting and briefly goes around for an introductory round, confirming attendees and establishing who is holding proxies. There are 17 full time attendees with Lepoint holding proxy for Halevi, Abe for Matsui (who joins at 14h) and Venkitasubramaniam, Stebila for Rosulek, and Abdalla for Lysyanskaya. Reyzin and Fischlin leave after lunch and Lepoint leaves at 15h40. Abdalla holds Lepoint's 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 12h30.

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); Nadia Heninger (Director 2019-2021); Tancrede 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); Mitsuru Matsui (*Asiacrypt'19* General Chair 2018-2019); Kenny Paterson (Journal of Cryptology Editor-in-Chief 2017-2019, *RWC* Steering Committee); Leo Reyzin (*Crypto'20* General Chair 2019-2020); Douglas Stebila (Membership Secretary 2017-2020).

Absentees (Elected). Shai Halevi (Director 2017-2019, *TCC* Steering Committee); Anna Lysyanskaya (Director 2019-2021).

Absentees (Appointed). Mike Rosulek (Communications Secretary);

Absentees (Representatives and Others). Kwangjo Kim, (*Asiacrypt'20* General Chair 2019-2020); Kevin S. McCurley (Database Administrator); Hilarie Orman (Archivist); Tal Rabin (Code-of-conduct Liaison); Marc Rotenberg (General Counsel); Muthu Venkitasubramaniam, (*Crypto'19* General Chair 2018-2019); 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 (virtual) Board meetings since *Crypto'18*. See a summary below.

Virtual meeting Virtual-1 '19 from 13 March 2019

- Board Meeting at *Eurocrypt'19*, Cachin, Find candidates for the position of Communications Secretary
Can be closed. This will be addressed in the current Board Meeting: see Section 3.2.
- 2020 IACR President, Find a new JoC Editor-in-Chief
Ongoing → new task.
- Board Meeting at *Eurocrypt'19*, LaMacchia, Stebila, Cachin, Work out the proposal to lower the registration fees and fund more student from excess income from last year.
This has been resolved → closed.
- Board Meeting at *Eurocrypt'19*, Paterson, Cachin, Halevi, Consult PCs and revise the current proposal for the journal-first track.
Ongoing → new task.
- Cachin, Appoint someone who will take the lead in drafting a statement addressing the US visa issues.
Ongoing → new task.
- Cachin, Collect names and then respond to the e-mail about recommending an cryptography and security editor for Arxiv.org.
This can be closed.

Virtual meeting Virtual-2 '18 from November 7, 2018

- LaMacchia, Stebila, Incorporate a feature in the registration system which can be used to track sponsorship payments even if they are made locally.
This has been done → closed.
- LaMacchia, Stebila, Bos, Addendum to GC guidelines to add the new sponsorship policy.
This has been done → closed.
- Cachin, Clarify the bylaws with respect to voting in the event of abstentions, quorum and unanimous decisions.
This is to be discussed at the current Board Meeting. See Section 5.1 → closed.
- Cachin, Create the Test-of-Time committee and appoint a chair and members.
This has been done → closed.
- Paterson, Halevi, Work out a proposal for journal-first submissions for discussion in the next Board meeting.
This has been done → closed.
- Abdalla (chair), Rose, Rogaway, Rabin, Standaert, Abe, Dunkelmann, Work out a first draft proposal how and if to proceed with the rolling co-chair model.
This is underway and can be closed, see Section 5.3.
- Cachin, Contact the Archivist to check in any tools used.
Ongoing → new task.

Minutes IACR Board Meeting Crypto'18 Santa Barbara, USA, 19 August 2018

- Cachin, Paterson, Update the JoC website to clarify the scope of the Journal regarding surveys and Systematization of Knowledge (SoK) papers.
Ongoing, should be done soon. → new task.
- Cachin, LaMacchia, Identify suitable candidates for sponsorship coordinator and possibly more generally for bookkeeping support.
Ongoing → new task.
- Rosulek, Finish the work on the news alert system.
Can be closed.
- Cachin, Preneel, Continue to talk to Springer to clarify which conferences are being considered for ISI indexing.
Ongoing → new task.
- Cachin, Preneel, LaMacchia, Find additional members for the audit committee (see Section ??).
Done → can be closed.
- Cachin, LaMacchia, Dunkelmann, Find additional members for the endowment committee.
Done → can be closed.
- End of September, Test-of-Time Committee, Update 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. Mail around for final approval and Board vote.
Done → can be closed.
- Cachin, Bos, Halevi, Lepoint, Rabin, Rose, Create a description of the code-of-conduct liaison role.
Open → new task.
- Cachin, Get feedback from our legal adviser on the current Code-of-Conduct.
Open → new task.
- Officers, Update the text in the budget spreadsheet to accommodate the affiliated events.
Done → can be closed.
- Cachin, Set-up a Doodle to select a date for the November Virtual Board meeting.
Done → can be closed.
- Rose, Contact and share information about the possibility to use a professional organizer for the affiliated events for *Crypto*.
Done → can be closed.
- LaMacchia, Investigate the benefits of doing outbound currency conversion wire transfers through a third-party service to reduce cost.
Done → can be closed.
- Halevi, Provide the program chair document from *TCC* to Rogaway.
Done → can be closed.
- Cachin, Rosulek, Stebila, Yu, McCurley, Converge on a concrete plan and timeline for the website modernization.
Done → can be closed.

- Rosulek, Cachin, McCurley, Get HSTS working for the IACR website.
Done → can be closed.
- Rosulek, Stebila, Work out the low-level details of integrating the membership database and news alerts (implemented by Rosulek).
Done → can be closed.
- Stebila, Add support to the conference registration system for closing registrations when limits have been reached and maintaining a waitlist.
Done → can be closed.
- Rosulek, Bos, Add the Code-of-conduct Liaison role to the Committees and Special Roles webpage.
Done → can be closed.
- Bos, Rosulek, Make sure that the election guidelines appear online.
Done → can be closed.
- Rogaway, Change text on policy on irregular submissions to make the punishment for plagiarism clearer.
Open → abandoned
- Cachin, Schedule an initial meeting with Marc Rotenberg (legal adviser).
Done → can be closed.
- LaMacchia, Rose, Rabin, Obtain additional quotes for the Directors and Officers insurance.
Done → can be closed.
- Rabin, Venkitasubramaniam, Fischlin, Dunkelman, Update the General-Chair guidelines.
Can be closed, see Section 5.2.
- LaMacchia, Cachin, Formalize the policy for affiliated events and workshops and make sure this gets added to the General Chair guidelines.
Done → can be closed.
- Preneel, Cachin, Rogaway, Halevi, Review and finalize the updated Program-Chair guidelines.
Partially done → can be closed.
- Cachin, Discuss publication of IEEE papers on the ePrint Archive with our legal counselor.
Can be closed.
- Lepoint, Deactivate the ePrint Archive forum, archive the messages and list the comments on a page linked to the relevant report.
Done → can be closed.
- all, Provide (minor) suggestions to Lepoint to improve the ePrint Archive.
Done → can be closed.

The new tasks are the following.

<p>Action Point 1: 2020 IACR President (<i>no time set</i>): Find a new JoC Editor-in-Chief</p>
--

<p>Action Point 2: Paterson, Cachin, Halevi (<i>Board Meeting at Eurocrypt'19</i>): Consult PCs and revise the current proposal for the journal-first track.</p>

<p>Action Point 3: Rose, Yung, Lysyanskaya (<i>no time set</i>): Create statement addressing the US visa issues.</p>

<p>Action Point 4: Cachin (<i>no time set</i>): Contact the Archivist to check in any tools used.</p>
--

<p>Action Point 5: Cachin, Paterson (<i>no time set</i>): Update the JoC website to clarify the scope of the Journal regarding surveys and Systematization of Knowledge (SoK) papers.</p>
--

<p>Action Point 6: Cachin, LaMacchia (<i>no time set</i>): Identify suitable candidates for sponsorship coordinator and possibly more generally for bookkeeping support.</p>

<p>Action Point 7: Cachin, Preneel (<i>no time set</i>): Continue to talk to Springer to clarify which conferences are being considered for ISI indexing.</p>
--

<p>Action Point 8: Cachin, Bos, Halevi, Lepoint, Rabin, Rose (<i>no time set</i>): Create a description of the code-of-conduct liaison role.</p>

<p>Action Point 9: Cachin (<i>no time set</i>): Get feedback from our legal adviser on the current Code-of-Conduct.</p>
--

1.5. Repetition of online votes 2019-1 and 2019-2. The Board needs to vote again on 2019-1 and 2019-2 since the number of votes received over e-mail did not reach a majority.

Decision 1 (Unanimous). *The Board approves the meeting minutes of Virtual-1 Board meeting in March 2019.*

Cachin thanks Bos for his work.

Decision 2 (Unanimous). *The Board approves proposal for TCC'20 in Durham, NC, selected by the TCC Steering Committee with general chair Alessandra Scafuro (North Carolina State University) and program chair Rafael Pass (Cornell, USA) and Krzysztof Pietrzak (IST Austria)*

1.6. Eurocrypt'19 Status. Fischlin gives an overview of the status of *Eurocrypt'19*. There are currently 544 registrations, this means the venue is virtually full and they cannot accept many more people. From the start they had an aggressive budget which aimed for a low registration fee and the General Chair is happy to see that this worked out. The affiliated workshops have in total 614 registrations. Everything is going fine and is under control. Cachin thanks Fischlin for his hard work.

2. OFFICER AND APPOINTEE REPORTS

2.1. Treasurer. LaMacchia presents the financial highlights of the year 2018 and for 2019 to date. In 2018 conferences made around USD 144K mainly due to *Crypto'18*. The 2018 non-conference income vs. expenses are a USD 25K deficit due to a negative USD 56K investment market value. We started using TransferWise for discounted currency conversions: this already saved over USD 19K since the beginning of 2019. The Treasurer recommends no change in membership fee.

LaMacchia wants to perform full audits on reports coming from the conferences but did not find time yet. Lepoint asks about the excess of income and how this can be used to reduce fees? The Treasurer explains that there is a budget set aside of USD 60k for student speakers. Moreover, there is a separate fund for USD 45k to lower registrations or offer additional student support. Bos asks if this budget is for all IACR venues. LaMacchia explains that this is for the flagship conferences only: for *Real World Crypto* the situation is different (more registrations leads to a bigger loss) and venues like *CHES* have sufficient sponsorship funding of their own.

Stebila asks how we book the currency conversion fees. LaMacchia explains that these costs are often hidden in the currency conversion itself. We have more clarity on this but it might not be worth the effort to separate this. The current conference planner does not contain an extra budget line for this information but the credit card fees are taken into account.

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. One of the ongoing discussion points is the journal first model, Paterson suggests to defer this to the *Crypto'19* Board meeting since Halevi is not present.

The number of outstanding pre-electronic submissions has been reduced from a starting figure of about 60 to 5. Currently there are 17 papers out for revision and 56 submissions under review: this is a fairly steady state. In the calendar year to date, we have received 66 submissions, of these 16 are currently under review. The remainder have been rejected, with the majority being immediately desk-rejected by the JoC EiC.

Paterson provides a brief summary of the Editorial Board changes and discusses the special issues. One special issue on TLS 1.3 will be announced this week and a special issue on the CAESAR competition was suggested by FSE Steering Committee.

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 in the repository. One of the major issues reported is that some authors seem to misuse the Conflict of Interest policy to cherry-pick reviewers. Also there is a strong preference for fewer sub-reviewers. Many of the suggestions require to invest more time to make the online reviewing tool better and add features.

There follows a discussion in the Board if we should switch to the HotCRP software for managing the conference review process. The advantages and disadvantages with impact for the IACR are discussed. This needs to be integrated with the IACR back-end and the President recommends that we need a senior volunteer who knows about the IACR processes for integration. Lepoint volunteers for the software system and Preneel volunteers to help with system level view.

Action Point **10: Lepoint, Preneel** (*no time set*):
 Modify the HotCRP software such that it integrates with the IACR back-end and perform a private dry-run.

2.4. **Membership Secretary.** Stebila presents an update on the membership composition. He points out that in 2019 we saw a significant membership increase to 2281 members so far due to *RWC*. We have 9 senior members for 2019.

The new membership system launched last August at *Crypto'18*. The new features include download receipts, attendee lists, and JoC subscription information. The transition to the new payment processor has been completed.

We continue to encounter “do_not_honor” credit card rejection for approximately 5 percent of registrants; this is due to our payment processor’s system and is out of our control. There follows a discussion about these rejections.

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. **Cryptology ePrint Archive.** The President recalls that Alexandra Boldyreva and Tancrede Lepoint are the current editors of the Cryptology ePrint Archive. Boldyreva has indicated she wants to step down. The President had started a search committee and Bos indicated he is willing to take over this role. The Secretary is asked to leave the room such that the Board can discuss this position.

Decision 3 (Unanimous). *Joppe Bos will replace Alexandra Boldyreva as the Cryptology ePrint Archive co-editor.*

3.2. **Communications Secretary.** The President recalls that Rosulek is stepping down as a Communications Secretary. The committee who looked for new candidates could not reach consensus. This position involves responsibilities for the communication to IACR members, the website and policies around this. The candidate needs some technical skills but McCurley offered to perform most of the technical work required for this position.

Several excellent candidates are nominated, and after discussion a candidate is selected.

Decision 4. *Foteini Baldimtsi will replace Mike Rosulek as Communications Secretary. [Baldimtsi subsequently accepted.]*

The President recalls the e-mail shared by McCurley where the progress was reported with respect to the modernization of the IACR webpage. The current revision of the website accomplishes a mobile-friendly version and a more modern and consistent look across the site. The Board is invited to try out the new webpage and is positively impressed with the new look and feel.

3.3. **Program and General Chair List Maintenance.** 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. There is a discussion about many names missing and how this is communicated to the Program Chairs. The Secretary agrees that the current version of the list need more input and would appreciate any input which the Board promises to provide. Preneel will make sure that these lists are shared with the Program Chairs. Heninger suggest that we ask the community for additional input to this list.

3.4. **Crypto '20–'21.** Daniele Micciancio has already been appointed as the Program Chair (rolling co-chair) for *Crypto'19* and *Crypto'20*. Several excellent candidates are nominated, and after discussion a candidate is selected.

Decision 5. *Tom Ristenpart is appointed Program Chair (rolling co-chair) for Crypto'20 and Crypto'21. [Ristenpart subsequently accepted.]*

3.5. **Asiacrypt '20–'21.** Shiho Moriai has already been appointed Program Chair (rolling co-chair) for *Asiacrypt'19* and *Asiacrypt'20*. Several excellent candidates are nominated, and after discussion a candidate is selected.

Decision 6. *Huaxion Wang is appointed Program Chair (rolling co-chair) for Asiacrypt'20 and Asiacrypt'21. [Wang subsequently accepted.]*

4. INTERNAL COMMITTEE APPOINTMENTS, REPORTS, AND DECISIONS

4.1. **Audit Committee.** Cachin reports that the audit committee has been formed and met at *Crypto'18*. A written report has been shared with the Board.

4.2. **Endowment Committee.** LaMacchia states that no proposal is ready for the investment policy but he recalls that Director and Officer insurance is now in place.

4.3. **Ethics Committee.** Rose gives a status update of the work performed by the Ethics Committee. He provides some insight in two cases which were brought to the attention of the Ethics Committee.

There is a discussion if and how we should clarify the Code of Conduct with respect to complaints which relate to events that occurred outside of the scope of IACR. Rose suggests that more people join the Ethics Committee to avoid possible conflicts such that cases can always be handled by 3 people from the committee.

Decision 7 (Unanimous). *The Ethics Committee will be enlarged with two more Board members to five members in total.*

Action Point 11: Bos (no time set):

Update the Policy for the Ethics Committee document with the correct names and the new size of the committee.

The Ethics Committee needs to find two additional members: Preneel and Batina subsequently volunteer to join this committee. The President thanks both of the new ethics committee members for volunteering.

There follows a discussion related to the Code of Conduct and if this applies to events or to the whole community as a whole (or both). It is discussed if and when we should ban members from IACR events.

Action Point 12: Bos, Rose (no time set):

Look into possible changes to the GC guidelines and the ethics committee policy to extend the scope of the Code of Conduct.

Fischlin asks what we can do in the short term. There follows a discussion how we should rethink our rules and policies.

4.4. **Schools Committee.** Abdalla recalls that the Schools Committee is looking for additional members since it is recommended that at least one of its members changes each year. Lepoint volunteers to join the committee which is approved by the Board and the Schools Committee will check internally if there is a volunteer to leave.

Abdalla states that a new chair is needed and the requirement that the chair must be a member of the Board is limiting the committee. He proposes to change this rule.

Decision 8. *The chair of the Schools committee does not need to be a member of the Board. However, there needs to be at least one board member on the Schools Committee which works in close liaison with the Board.*

Action Point 13: Bos (no time set):

Update the Schools Committee policy to reflect the decision taken with respect to the chair.

Action Point 14: Bos (no time set):

Update the webpage with the new members of the Schools Committee.

There is a discussion about organizing Schools in regions where we cannot send money such as Iran. At the moment it seems not possible to organize Schools there. Currently the Schools Committee is waiting for the June 30 deadline. The President goes over the list of schools proposals and encourages the committee for more advertisement.

4.5. **Test-of-Time Award Committee.** The President recalls that the committee has made the first decisions for the Test-of-Time awards. The winners have been announced and the first ones will be honored at *Eurocrypt'19*.

Action Point 15: Test-of-Time Committee (*Crypto'19*):

Appoint new members to the Test-of-Time Award committee.

4.6. **Code-of-conduct Liaison.** No update or report has been received by the Code-of-Conduct Liaison.

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 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 changes and impact have been shared before the meeting and are presented by the President during the meeting.

There is a brief discussion about this change and the impact. Preneel is concerned that a majority can be reached too easily in the virtual board meetings which are called on minimal short notice and suggests to increase the quorum to 2/3 of the members of the board. The Presidents calls first the increase to 2/3 for a vote and next the combined changes.

Decision 9. *The Board agrees to amend the text in Article V: Board of Directors in the bylaws:*

“A majority of the Board (including proxies) constitutes a quorum at the meetings. Decisions are made by a majority vote of the Directors present (including proxies) at meetings or by a majority vote of all members of the Board for actions taken outside of the meetings.”

to:

“More than 2/3 of the members of the Board (including proxies) constitutes a quorum at the meetings. Decisions are made by a majority vote (including proxies) at meetings or by a majority vote of all members of the Board for actions taken outside of the meetings.”

This proposed amendment will be put forward to the members in a referendum.

Related to the amendment, the term “full Board” in Article XVI of the bylaws is discussed.

Action Point **16: Bos, Rose** (*no time set*):
Clarify what the term “full board” exactly means.

5.2. Update of General-Chair guidelines. The President recalls that the General-Chair guideline still needs work especially regarding the organization of affiliated events. Due to time constraints this is not discussed further.

Action Point **17: President** (*no time set*):
Update the General-Chair guidelines regarding the organization of affiliated events.

5.3. Update of Program-Chair guidelines. The President recalls the discussion we had in the previous Board Meetings with respect to program chair model. Abdalla summarizes the plan for alternative models, especially the parallel co-chair idea. Currently, the load is substantial for chairs and some feel that the current rolling co-chair model might not have solved this. The downside of the parallel co-chair model is that some members think that we are not able to fill the pipeline of chairs: this applies to Asiacrypt but also to Crypto to represent chairs from all disciplines in cryptology. The committee which looked at this did not reach agreement. Abdalla suggests to conduct a survey with IACR members. There is general disagreement on the Board if this will be effective. Paterson points out that we are elected to make such decisions. Standaert suggests to ask previous chairs but Preneel points out this was already done and the response was mixed. The President suggests to defer this discussion to a future Board meeting.

6. CONFERENCES

6.1. Affiliated workshops at conferences. Cachin reminds the Board that a policy for affiliated events is still needed. An update is being made to the conference planner.

Fischlin provided feedback about his experience when organizing affiliated events. A first question is who approves the workshop chair(s)? The President recalls that a workshop chair is named in the original proposal. This information should be included in the General Chair guidelines. The workshop chair needs to report to the General Chair of the event.

Action Point **18: Bos** (*no time set*):
Update the GC guidelines with workshop chair information. This person needs to report to the GC which in case of dispute decided.

Action Point **19: LaMacchia, Cachin** (*no time set*):
Finish the update of the conference planner regarding the budget of workshops.

There follows a discussion about how we should handle the registration cost for affiliated events. Yung put forward that this is up to the GC to handle this. LaMacchia points out that this should comply with the IACR policy: the Board agrees.

Action Point **20: Preneel** (*no time set*):
Draft text for a workshop proposal, this needs to include the CoI. Possibly use Batina’s proposal.

The President thanks Fischlin for his useful suggestions.

7. CONFERENCE REPORTS SINCE LAST BOD MEETING

7.1. Asiacrypt’18. The event was a success. Nothing special to report.

7.2. Crypto’18. Nothing to report.

8. FORTHCOMING CONFERENCES

8.1. **Crypto'19.** *Crypto'19* will be held at UCSB from August 18-22. Since Venkitasubramaniam is not present there is no update.

Action Point **21: President** (*no time set*):
Check with Venkitasubramaniam for the affiliated events.

8.2. **Asiacrypt'19.** Matsui explains that the organization for *Asiacrypt'19* is going well. The budget plan has been submitted. The Presidents inquires about the organization of affiliated events. Matsui explains that this is not planned. The President looks forward to *Asiacrypt'19*.

8.3. **Eurocrypt'20.** Batina gives a status update on *Eurocrypt'20*. Everything is going as planned, she has visited the venue in October. The room can host up to 700 people and can be split in two separate rooms of 1/3 and 2/3 of the capacity. Moreover, Zagreb Airport is being renovated. Schwabe serves as the workshop chair and the call for workshop proposals is out. Reserved for the affiliated events are 8 rooms in the hotel and 8 additional ones in the university.

9. EVENT PROPOSALS, GENERAL CHAIR APPOINTMENTS, AND STEERING COMMITTEE REPORTS

9.1. **Asiacrypt '21 proposal and general chair appointment.** Jian Guo presents a proposal for *Asiacrypt'21* in Singapore, which has already been selected by the Asiacrypt Steering Committee. The plan is to have *Asiacrypt'21* from December 5 to 9. Cachin thanks Guo for this proposal.

Decision 10 (Unanimous). *The proposal for Asiacrypt 2021 in Singapore is accepted, with Jian Guo as General Chair.*

9.2. **Eurocrypt '21 proposal and general chair appointment.** Colin Boyd present a proposal for *Eurocrypt'21* in Trondheim, Norway. There are some questions about the proposed dates: having the conference in either late April or late May or even the beginning of June.

Decision 11 (Unanimous). *The proposal for Eurocrypt 2021 in Trondheim, Norway is accepted, with Colin Boyd as General Chair. The exact dates should be discussed again.*

9.3. **CHES Steering Committee.** The slides for the *CHES'20* proposal are in the repository. The CHES steering committee is currently discussing if they should switch to dual-track conference.

9.4. **FSE Steering Committee.** Preneel recalls that we need to vote on the proposal for *FSE'21* in Beijing, China. The proposal has been shared for the meeting and can be found in the repository.

Decision 12 (Unanimous). *The proposal for FSE'21 in Beijing, China is accepted, with Bin Zhang as General Chair.*

9.5. **PKC Steering Committee.** Nothing to mention: *PKC'20* will take place in Edinburgh.

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

9.7. **TCC Steering Committee.** No updates, the Board just approved *TCC'20* in Durham, NC, selected by the TCC Steering Committee.

9.8. **Schools Committee (Cryptology Schools).** The Schools Committee recalls that we have budget for schools. No update since the deadline is coming up in June.

10. CLOSING MATTERS

Abdalla recalls that he was asked by Lysyanskaya to bring up another issue. Currently, Section 4 of the Program Chair guidelines states that "For Asiacrypt, Crypto, and Eurocrypt it is recommended that a PC member is single author for at most one submission or co-author for at most two submissions (not both)." Lysyanskaya suggests to increase the number of submissions per PC member to three. Bos and Cachin recall that this rule was recently relaxed from one submission to two with co-authors to accommodate situations where PC-members have submissions with students. Heninger wonders if we need any restrictions since we have a Conflict-of-Interest policy in place. Preneel is against changing this since we need to avoid situations where mainly PC members get papers accepted even if these papers are good: this simply looks bad. Yung agrees, based on past experience no rules on PC-member submissions results in a significantly increase of PC-members accepted papers.

Abdalla wants to bring this to a vote which subsequently fails.

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

- the affiliated events
- possible change of start and end day for the conferences
- visa problems

10.2. **Review of Action Points.** After a brief review of action points, Cachin closes the meeting at 17h35.