MINUTES IACR BOARD MEETING *CRYPTO'18*

SANTA BARBARA, USA, 19 AUGUST 2018

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. Yung, Abdalla, and Fischlin join the meeting at 10h12 while Paterson joins only for the Journal of Cryptology reporting.

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). The topic of affiliated events is added to the agenda by LaMacchia (see Section 5.4). These minutes are reordered to the original agenda for consistency.

Rabin asks why we do not receive a printed version of the agenda. Bos explains that the agenda is shared before the meeting in electronic form: the President has mailed this around and this can be found in the IACR repository.

1.2.1. *Roll of Attendees.* There are 20 full time attendees with Yung holding proxy for Standaert, LaMacchia for Dunkelman, Rose for Preneel (during the time he is not present) and Abdalla for Paterson. LaMacchia is present as the *RWC* Steering Committee representative.

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

Attendees (Appointed). Marc Fischlin (*Eurocrypt'19* General Chair 2018-2019); Mitsuru Matsui (*Asiacrypt'19* General Chair 2018-2019); Tal Rabin (*Crypto'18* General Chair 2017-2018, Code-of-Conduct Liaison); Mike Rosulek (Communications Secretary); Douglas Stebila (Membership Secretary 2017-2020); Muthu Venkitasubramaniam, (*Crypto'19* General Chair 2018-2019).

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

Absentees (Elected). Francois-Xavier Standaert (Director 2017-2019, *CHES* Steering Committee);

Absentees (Appointed). Orr Dunkelman (*Eurocrypt'18* General Chair 2017-2018); Kenny Paterson (Journal of Cryptology Editor-in-Chief 2017–2019, *RWC* Steering Committee); Josef Pieprzyk (*Asiacrypt'18* General Chair 2017-2018);

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

1.3. **Approve minutes from last BoD meeting and membership meeting.** The *Eurocrypt'18* Board meeting minutes have already been approved and published online. Cachin thanks Bos for finishing the minutes in a timely manner.

1.4. **Review of Open Action Points.** Bos briefly reviews the status of action items identified from the *Eurocrypt'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. Update the JoC website to clarify the scope of the Journal regarding surveys and Systematization of Knowledge (SoK) papers.*
  No progress, new action item has been defined.
- *Rogaway. Collect reports from program chairs of conferences of last 2 years and ask them about the work load in this model.*
  Done.

- *Preneel. Update the PC guidelines to include the ToSC hybrid model and the relationship between Transactions on Symmetric Cryptology and Journal of Cryptology.*
  Done, needs review. See Section 5.5.
- *Cachin, LaMacchia. Identify suitable candidates for sponsorship coordinator and possibly more generally for bookkeeping support.*
  No progress, new action item has been defined.
- *Cachin, Paterson. Sort out how to handle best papers for ToSC and TCHES in relationship with the JoC.*
  Done. The steering committees decided not to send the best papers to JoC.
- *Rosulek. Finish the work on the news alert system.*
  Partially completed. New action item has been defined.
- *Cachin, Preneel. Continue to talk to Springer to clarify which conferences are being considered for ISI indexing.*
  Ongoing, initial discussions have taken place. New action item has been defined.
- *Abdalla. Complete the financial summary of Eurocrypt'17 and provide this to the treasurer.*
  In progress. Item can be closed.
- *Cachin, Preneel, LaMacchia. Find additional members for the audit committee.*
  No progress, new action item has been defined.
- *Cachin, LaMacchia, Dunkelman. Find additional members for the endowment committee.*
  No progress, new action item has been defined.
- *Schools Committee. Discuss new membership for the Schools Committee for 2018.*
  Done.
- *Cachin. Make initial contact with Rotenberg.*
  Done.
- *Test-of-Time Committee. 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.*
  No progress due to the organization of *Crypto'18*. New action item has been defined, see Section 5.1.
- *LaMacchia. Share the quotes for the Directors and Officers insurance when they are available.*
  In progress, one quote has been received and is available in the svn. This was higher than expected, more investigation is needed. New action item has been defined in Section 5.2.
- *Stebila. Add the new Code of Conduct to the webpage template.*
  Done.
- *Cachin, Bos, Halevi, Lepoint, Rabin, Rose. Create a description of the code-of-conduct liaison role.*
  Ongoing, new action item has been defined.
- *Cachin. Get feedback from our legal adviser on the current Code-of-Conduct.*
  No progress, need to establish initial contact with the legal adviser. New action has been defined.
- *Cachin, Rabin, Fischlin. Coordinate to update the General Chair guidelines.*
  This item is merged with the new action item defined in Section 5.3.
- *Cachin, Rogaway, Fischlin. Coordinate to update the Program Chair guidelines.*
  This has been completed by Preneel when adding information related to the hybrid model, see Section 5.5. Done.
- *Officers. Update the text in the budget spreadsheet to accommodate the affiliated events.*
  No progress. New action has been defined.
- *Cachin. Continue this discussion with the entire Board over e-mail related to the number of physical and virtual Board meetings.*
  It has been decided that another virtual Board meeting will take place in November, see action item below. This item is closed.

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

Action Point **3: Rosulek** *(no time set)*:
Finish the work on the news alert system.

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, Preneel, LaMacchia** *(no time set)*:
Find additional members for the audit committee (see Section 4.2).

Action Point **6: Cachin, LaMacchia, Dunkelman** *(no time set)*:
Find additional members for the endowment committee.

Action Point **7: Test-of-Time Committee** *(End of September)*:
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.

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

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

Action Point **10: Officers** *(no time set)*:
Update the text in the budget spreadsheet to accommodate the affiliated events.

Action Point **11: Cachin** *(no time set)*:
Set-up a Doodle to select a date for the November Virtual Board meeting.

1.5. ***Crypto'18* Status.** Rabin gives an overview of the status of *Crypto'18.* There are 635 confirmed attendees for *Crypto'18*, 860 attendees when including the affiliated events, and over 1200 daily registrations. This is a new record and the setup with the affiliated events is a huge success. We received USD 140k in sponsorship of which USD 50k was used to sponsor students. Around 30 percent of all registrations are student registrations for *Crypto'18.*

UCSB did not assist with the registrations of the affiliated events. This is a significant effort: how to handle this in the future? This is hard to arrange when you are not local at UCSB. The President recalls we no longer have a formal relationship with UCSB, we need to discuss how to handle this for upcoming events.

Rabin explicitly thanks Fabrice Benhamouda and Elette Boyle for their incredible amount of work to make *Crypto'18* and the affiliated events such a big success.

The Treasurer asks about meal ticket money which has been coming in over the last couple of days. Rabin explains that when attending the affiliated events the attendees received meal vouchers which were purchased in bulk to avoid long lines at the cafeteria. The cafeteria counts the vouchers used. Attendees to *Crypto'18* who are not staying in the dorms need to purchase lunch vouchers or pay by credit card at the cafeteria. The Treasurer points out that we do not take these credit card charges into account in the budget.

Rose points out the he knows a local professional organizer who might be able to assist in the future for the affiliated events for *Crypto*. Cachin agrees that offloading this work to a workshop chair is a good idea.

Action Point **12: Rose** *(no time set)*:
Contact and share information about the possibility to use a professional organizer for the affiliated events for *Crypto*.

Rabin thanks Stebila for his assistance with the registration process on the IACR webpage. Cachin thanks Rabin for her hard work and making *Crypto'18* such a success by breaking registration records.

2. Officer and Appointee Reports

2.1. **Treasurer.** LaMacchia presents the financial report up to the end of the first half of 2018. The final financial reports of *Eurocrypt'17*, *Crypto'17*, and *TCC'17* are overdue. As of the end of July 2018, the IACR assets are roughly USD 2.66M. The cash flow over last 12 months was almost USD 1.5M. Since moving to Stripe we have processed USD 1.7M in transactions with an average fee of 2.4 percent (down from 5.9 to 6.2 percent).

A small number of people have reported problems with Stripe, the problem seems to be a bank problem. This explains the increase for wire transfers. An explanation is a possible misclassification of our merchant code or potentially because we have "crypto" in our name (it seems some banks block these transactions due to links with currency conversion to cryptocurrencies).

We are spending more funding on student speaker waivers. Rabin asks what happens with soft merges and both papers have a student speaker. LaMacchia explains that indeed both speakers will receive waivers. A frequently asked question is who exactly can receive these student speaker waivers. The current approach is that all PhD students and students who just finished their Master and still need to begin their PhD are eligible. In general, post-docs are not eligible.

The Treasurer would like to investigate the possibility of doing outbound currency conversion wire transfers through a third-party service to reduce cost. The Board agrees this is an excellent idea.

Action Point **13: LaMacchia** *(no time set)*:
Investigate the benefits of doing outbound currency conversion wire transfers through a third-party service to reduce cost.

Transferring funds to India continues to be extremely difficult and unpredictable. Sponsorship invoicing through registration system appears to be working well. The Treasurer thanks Stebila for his work in enabling this.

The Treasurer is required to make a recommendation regarding the membership fee and sees no reason to change this. The Treasurer suggests to open an addition bank account for the expenses of *Crypto'19* and add the General Chair as a signatory.

Decision 1 (Unanimous)**.** *The BoD approves the opening of an additional checking account at 1st Security Bank of Washington for the use of the Crypto'19 conference with Venkitasubramaniam and LaMacchia as signatories.*

Rogaway asks for more details about our current investments. The investment are under discussion with the endowment committee, but given the other higher priority tasks of LaMacchia this is likely to be pushed into the future. Cachin thanks LaMacchia for the enormous amount of work he has done.

2.2. **JoC Editor in Chief.** Paterson shared his written report before the meeting. He explains that he took over as Editor-in-Chief on January 1st 2017, taking on responsibility for all existing submissions in the online submission system. Working with the President and Matt Franklin (former EiC), the number of outstanding pre-electronic submission have been reduced from a starting figure of about 60 to 9.

The year 2017 closed with a total of 145 submissions. In the calendar year to date, we have received 120 submissions (so we can expect a total of about 180 this year). Of these, 21 are currently under review. The remainder have been rejected, with the majority being immediate desk rejects by the current Editor in Chief, and a small number being quickly rejected by the assigned associate editor.

The best papers of the three general conferences plus *PKC* and *TCC* are still invited to the JoC. However, the "25 percent rule" (requiring 25 percent new material in submissions) for JoC together with the increased page size limits for the conferences has the effect that the full-version is often published at the conference. *FSE* and *CHES* decided to no longer make best paper recommendations to the JoC. Rabin remarks that this essentially prevents these communities to submit to the JoC. Bos points out that this is not necessarily true since people can directly submit to the JoC. Cachin and Yung explain that this effect was predicted in the past and was an active decision. Rabin informs about the impact on the number of submissions. Paterson explains that the impact is limited since papers from the CHES community were often not submitted to the JoC.

Paterson explains that his 3-year term of appointment will end in December 2019 and that he currently is half way through. Cachin asks if we can convince him to stay.

Venkitasubramaniam asks if we invite other papers to the JoC besides the best papers. This does not happen at the moment and is considered a good idea by the Board. Lysyanskaya asks if people submit directly to the JoC. Paterson explains that this does happen especially with the recent shorter time for papers to get reviewed.

2.3. **Program chair contact.** Rogaway explains that very few PC reports have been received although this is a mandatory part of being a PC. Cachin wonders how we can improve communication between the Board and the PCs? Rogaway is confident that more reports will be submitted to the Board. Halevi explains that *TCC* keeps a Google document with useful information for the new PC by previous PC.

Action Point **14: Halevi** *(no time set)*:
Provide the program chair document from *TCC* to Rogaway.

The question is raised if we should take action if authors withdraw their paper after a first round of (negative) review. Cachin explains that this is not something we currently forbid and does not see a problem.

2.4. **Communications Secretary.** Rosulek explains the shared report. Work on the news alert system has been performed: this now has a web-based administration interface. The identified action items are recalled below. Cachin thanks Rosulek and Yu for their work and progress.

Action Point **15: Cachin, Rosulek, Stebila, Yu, McCurley** *(no time set)*:
Converge on a concrete plan and timeline for the website modernization.

Action Point **16: Rosulek, Cachin, McCurley** *(no time set)*:
Get HSTS working for the IACR website.

Action Point **17: Rosulek, Stebila** *(no time set)*:
Work out the low-level details of integrating the membership database and news alerts (implemented by Rosulek).

2.5. **Membership Secretary.** Stebila presents an update on the membership composition. It seems likely we will exceed 2000 members for membership year 2019 due to *RWC* and the increased attendance of *Crypto'18*. The code of conduct has been added to to registration form. Stebila shows the new features which has been added to the membership system. He points out that we still need to figure out how to deal with conferences which reach capacity and use a wait list.

Action Point **18: Stebila** *(no time set)*:
Add support to the conference registration system for closing registrations when limits have been reached and maintaining a waitlist.

The entire Board thanks Douglas for all his work including all the support for *Crypto'18*.

2.6. **Code-of-conduct Liaison.** Rabin summarizes that one issue has been reported. This was resolved effectively and we responded quickly. Rabin assisted in drafting a letter to the ethics committee. This was received by the filing party as very positive.

Action Point **19: Rosulek, Bos** *(no time set)*:
Add the Code-of-conduct Liaison role to the Committees and Special Roles webpage.

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.

3.2. ***Eurocrypt '20-'21* Program Co-Chair appointment.** Yuval Ishai is already appointed Program Chair (rolling co-chair for *Eurocrypt'19* and *Eurocrypt'20*). Several excellent candidates are nominated, and after discussion a candidate is selected.

Decision 2. *Anne Canteaut is appointed Program Chair for Eurocrypt '20-'21 (rolling co-chair for Eurocrypt'20 and Eurocrypt'21). [Canteaut subsequently accepted.]*

3.3. **Distinguished Lecturer '20 (to be held at *Crypto*).** The distinguished lecture is held annually, on invitation by the Board. Its location cycles between the three main IACR conferences. Several excellent candidates are nominated, and after discussion a candidate is selected.

Decision 3. *Silvio Micali is invited to deliver the Distinguished Lecture at Crypto'20. [Micali subsequently accepted.]*

3.4. ***Crypto'20* General Chair.** Several excellent candidates are nominated, and after discussion a candidate is selected.

Decision 4. *Leo Reyzin is appointed General Chair for Crypto'20. [Reyzin subsequently accepted.]*

4. Internal Committee appointments, reports, and decisions

4.1. **Fellows Committee.** Lysyanskaya informs the Board that not much is to be reported since the Board meeting at *Eurocrypt*. She recalls that there is a small anomaly in the committee since there is no-one which has served five years and two members serve three years. This has been addressed and is resolved.

Currently, the text of the Fellow Program states that "The total number of Fellows to be selected in any one year is expected to be approximately 0.25% and should not exceed 0.5% of the current total membership." However, given the amount of fellow nominations Lysyanskaya points out we maybe should modify the text to "The total number of Fellows to be selected in any one year is expected to be approximately between 0.25% and 0.5% of the current total membership." since currently the aim has always been to achieve 0.25 percent of the current total membership. Cachin leaves this proposed modification to the discussion within the Fellows Committee.

Cachin thanks Lysyanskaya for her work on the Fellows Committee.

4.2. **Audit Committee.** Cachin recalls that forming the audit committee is still an open action item. Rose informs the President that if the IACR has a turnover over two million USD then an audit by an external auditor is mandatory[1]. We need to form the audit committee and be prepared.

[1] After further investigation after the Board meeting Rose reports that we do not need to have an audit if we exceed USD 2M; this is a rule for California-based non-profits but since the IACR is a Nevada-based non-profit this rule does not apply (and Nevada does not have such a rule).

4.3. **Endowment Committee.** Nothing to report. Action item is still ongoing.

4.4. **Election Committee.** Abe reports that the Election 2018 webpage has been created. A mismatch between the bylaws and the election guidelines in terms of stated dates has been identified and the guidelines have been updated.

Action Point **20: Bos, Rosulek** *(no time set)*:
Make sure that the election guidelines appear online.

4.5. **Ethics Committee.** Rose presents the report he has shared with Board before the meeting. The case of harassment at *RWC* has been taken care of. Rose recalls this incident was the reason why we created the Code-of-Conduct. There has been a plagiarism case and after investigation the authors are banned to submit to any IACR conference for one year. There follows a discussion if we should write to the university which employs these authors. Yung stresses that if we do this then it is to deter others and we should bring this case to the public such that it is known. Halevi states that plagiarism violates the trust of scientists, there need to be a real punishment.

Action Point **21: Rogaway** *(no time set)*:
Change text on policy on irregular submissions to make the punishment for plagiarism clearer.

There has been one case of harassment reported through the code-of-conduct liaison of young B by more senior A. Possible actions are discussed and the Ethics Committee will follow-up.

There was a request if cryptocurrencies should be explicitly mentioned in the Conflict-of-Interest policy. Everyone agrees that since the CoI already mentions financial interests this is covered. We leave the CoI text as-is.

4.6. **Schools Committee.** Three requests for School funding have been received by the School Committee. Abdalla gives a summary of the Committee's findings and recommendation. The Board decides to fund the two schools as recommended by the School Committee.

Decision 5 (Unanimous)**.** *The Board adopts the proposal by the Schools Committee, meaning that the The 1st Crypto Innovation School (CIS 2018) (November 29th-December 1st, 2018, Shenzhen, China) will be supported with USD 9.5k and the Australian Summer School on Embedded Cryptography (9-11 December 2018, The University of Adelaide, Adelaide, Australia) will be supported with AU$ 6K.*

One issue is discussed where a previous school promised to increase the diversity of the speakers but they did not act on this. It is hard to impose measures after the school has taken place but this fact will be taken into account will the organizers ever request funding for a school again.

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. Cachin will re-initiate contact and involve the Officers and Lysyanskaya and schedule a meeting.

Action Point **22: Cachin** *(no time set)*:
Schedule an initial meeting with Marc Rotenberg (legal adviser).

5. Procedures, Bylaws and Guidelines

5.1. **Test-of-time award.** Rabin (chair of the Test-of-Time Committee) reports that no progress has been made. See the continued action item earlier: Rabin will 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. This will be mailed around for final approval and Board vote within a month (end of September).

5.2. **Directors and Officers insurance.** Cachin recalls the plan to obtain a Directors and Officers insurance. LaMacchia reports that a first offer has been obtained but more are needed to make a decision. Rose volenteered to assist and Rabin promises to also get an offer for this D&O insurance.

Action Point **23: LaMacchia, Rose, Rabin** *(no time set)*:
Obtain additional quotes for the Directors and Officers insurance.

5.3. **Update of General-Chair guidelines.** Cachin has identified multiple issues in the General-Chair guidelines due to historical reasons. After a discussion it becomes clear previous GCs would like to add other useful information as well.

Action Point **24: Rabin, Venkitasubramaniam, Fischlin, Dunkelman** *(no time set)*:
Update the General-Chair guidelines.

5.4. **Affiliated events.** LaMacchia has mailed around an issue related to the organized affiliated events. He asks if for purposes of recording, publication and dissemination of talk-related materials the affiliated events are official "IACR Events" or independent activities? Multiple conflicts with existing IACR policies have been identified in case they are IACR events, in case they are independent of the IACR we should not be involved in distribution of materials.

Cachin expresses that he is in favor of the affiliated events. Preneel suggest we mention this explicitly in our policies. Cachin agrees that if we do the registration then the event should follow the rules and regulations of an IACR Event. This needs to be added to the guidelines and an item needs to be added to the Budget forms (action item already defined).

Action Point **25: LaMacchia, Cachin** *(no time set)*:
Formalize the policy for affiliated events and workshops and make sure this gets added to the General Chair guidelines.

5.5. **Update of Program-Chair guidelines.** Cachin recalls that multiple issues have been identified in the Program-Chair guidelines due to historical reasons and a revision is needed. These changes have been performed already by Preneel when going over the document when including the ToSC hybrid model and the relationship between Transactions on Symmetric Cryptology and Journal of Cryptology.

Action Point **26: Preneel, Cachin, Rogaway, Halevi** *(no time set)*:
Review and finalize the updated Program-Chair guidelines.

6. CONFERENCES

6.1. **Discuss rolling co-chair model for program chairs.** Rabin presents the slides on the work performed by Abdalla, Rabin, Rogaway to collect past chairs' feedback on workload and the rolling-chair model.

This model has a number of disadvantages: the workload is quite high to do this for two years, synchronization seems to create more work, especially when chairs don't have complementary expertise, and there is often a topic imbalance between researchers in America, Asia, and Europe. This makes it difficult to find suitable chairs for the general conferences with broad, complementary expertise. Moreover, Rabin highlights that a lot of young people want to become program chair with an eye on their career. Currently, the program chairs are often more senior cryptographers. Rabin suggests that we move to a (parallel) two-chair model per year since this increases the number of new chairs per year and removes the raised concern about the two-year commitment.

The Board discusses if being asked to serve as a program chair can be considered an "award" and if this is really taken into account when people are up for promotion. Stories are shared which highlight examples where this helped and cases where this did not matter. LaMacchia recalls that from an industrial point of view this is purely a service to the community. He suggests that appointing an associate program chair might reduce the workload. Preneel wonders why we do not merge the two ideas and create a rolling co-chair model but with dedicated area chairs.

Yung suggests the Board votes on a motion to change the current rolling co-chair model to a model where we change the two PCs every year. Cachin highlights we have to plan this carefully. When we make sudden changes we need to ensure we put a smooth transition phase in place. Rogaway states he strongly disagrees with some of the previous arguments to change the current model: being PC is not considered an award and we have a hard time finding good people for this job. Hence, he sees no valid motivation to change the current way of working. Rose sees a potential risk since selecting two random people every year and force them to work together is asking for potential disasters. Halevi disagrees and does see being a PC as an award, thinks we have sufficient good people, and this new model has worked well for some of the area conferences.

Cachin highlights that if we propose to change anything this should hold for all three general conferences. He welcomes the current discussion but the received feedback from the previous PCs is not very clear on their preferences. Rogaway asks what is exactly broken in the current model. Halevi explains that the problem is related to the workload and the pipeline of new PCs. Stebila agrees that there are problems with the current model but that the current proposal is not ready to be voted on. Preneel asks again why we don't go for a short-term solution first where we use area chair before we decide to make a larger change. Yung demands the Board votes on a motion which pursues further work towards changing the rolling co-chair model to parallel co-chair. After a voting round this proposal is dismissed. Bos suggests to change the proposal such that the scope is broader.

Decision 6. *The Board will pursue further work towards changing the rolling co-chair model for the general conferences.*

7. Publications

7.1. **Cryptology ePrint Archive.** Cachin recalls there always have been minor and major issues with the ePrint Archive. Lepoint presents an overview of statistics: there are about 1250 reports per year since 2015.

There might be a problem with accepting IEEE papers on ePrint. Prior to submission to IEEE there is no issue but this might be not allowed upon submission. This is something we need to discuss with our legal counselor since this needs to be clarified.

> Action Point **27: Cachin** *(no time set)*:
> Discuss publication of IEEE papers on the ePrint Archive with our legal counselor.

Lepoint proposes to perform a manual clean-up: this includes for instance the encoding of the authors names. Hence, this manual clean-up does not modify the scientific content but modifies the archive itself. Cachin wonders if such changes might upset crawlers but this seems unlikely.

The number of posts to the forum has been declining every year and the last two years there were only two post per year. Lepoint notes that the forum is not linked to IACR registration, uses an external system and the software has not been updated for years. He proposes to deactivate the forum and archive the current posts.

Decision 7 (Unanimous)**.** *The Cryptology ePrint Archive discussion forum will be deactivated and the current posts will be archived.*

> Action Point **28: Lepoint** *(no time set)*:
> Deactivate the ePrint Archive forum, archive the messages and list the comments on a page linked to the relevant report.

Lepoint is willing to perform minor modifications to improve the archive and solicits for more input.

> Action Point **29: all** *(no time set)*:
> Provide (minor) suggestions to Lepoint to improve the ePrint Archive.

Cachin thanks Lepoint for all his work on improving the ePrint Archive.

8. Conference reports since last BoD Meeting

8.1. ***Eurocrypt '18.*** Dunkelman has shared a preliminary report on *Eurocrypt '18*. There were 379 full attendees, and another 20 who registered to the bitcoin session. One thing to note is that we had many late registrations. Slightly more than 100 attendees have registered after the deadline. All in all, the conference went relatively smoothly.

9. Forthcoming Conferences

9.1. ***Asiacrypt '18.*** There has been a status update from Pieprzyk for *Asiacrypt'18*. The *Asiacrypt'18* call for papers is out. Everything is going as planned. The Treasurer expects to sign off on the budget soon.

9.2. ***Eurocrypt'19.*** Fischlin gives a status update on *Eurocrypt'19*. Everything is going as planned. For *Eurocrypt'19* there is a conflict of dates with the 40th IEEE Symposium on Security and Privacy. Both events are always around the same dates and we should keep in mind and verify that such overlap does not occur again in the future. The planning of the affiliated events is delegated to two post-docs, this will take place the weekend before *Eurocrypt*. Stebila raises the issue that just as with *Crypto'18* the affiliated events will take place during the Board meeting. The President offers that we do not neccesairy have to start the conference on Sunday evening. Rabin suggests to have the affiliated events bi-yearly. Cachin does not support this suggestions and expresses that continuity is crucial. Yung and Venkitasubramaniam also express that the affiliated events are a great success and we should keep them every year.

9.3. ***Crypto '19.*** Venkitasubramaniam is preparing by learning from Rabin how *Crypto'18* is being organized.

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

10.1. **CHES Steering Committee.** Cachin summarizes the report shared by Standaert. *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*.

10.2. **FSE Steering Committee.** Preneel explains that the preparations for *FSE'19* (Paris, France in March 25-28 2019) are on track. The Board needs to appoint the Editor-in-Chief (Program Chair) for Transactions on Symmetric Cryptology for the year 2019.

Decision 8 (Unanimous)**.** *The Board follows the proposal by the FSE Steering Committee and appoints Gaëtan Leurent as the Editor-in-Chief (Program Chair) for the Transactions on Symmetric Cryptology for the year 2019.*

10.3. **PKC Steering Committee.** Yung informs the Board that the webpage for *PKC'19* (April 14-17, 2019 Beijing, China) is up and running. There is nothing much to report.

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

10.5. **TCC Steering Committee.** Halevi recalls that *TCC'18* takes place in India on November 11-14, 2018. Everything is going fine. There is not much to report.

11. Closing Matters

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

- actions by the ethics committee
- workshop and affiliated events
- the discussion related to the rolling co-chair model

11.2. **Review of Action Points.** After a brief review of action points, Cachin closes the meeting at 17h49.