MINUTES IACR BOARD MEETING *CRYPTO'17*

UCSB, SANTA BARBARA, 20 AUGUST 2017

1. Opening Matters

1.1. **Welcome, roll of attendees, identification of proxies.** At 10:09 Cachin opens the meeting and he briefly goes around for an introductory round, confirming attendees and establishing who is holding proxies. Dunkelman arrived at 10h19 and Abdalla arrived at 10h34.

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. The topic proposed by Rabin on appointing Program Chairs was added to "Procedures, bylaws and guidelines", the topic proposed by Rose on Visa issues was added to "Conferences" and the topic proposed by Preneel on ISI+LNCS was added to "Publications". There was an adjournment for lunch around 13h.

1.2.1. *Roll of Attendees.* There are 17 attendees with Benaloh holding proxy for LaMacchia, Rabin for Halevi, Rogaway for Paterson, and Myers for Rosulek.

Attendees (Elected). Christian Cachin (President 2017-2019); Greg Rose (Vice President 2017-2019); Joppe Bos (Secretary 2017-2019);

Michel Abdalla (Director 2016-2018, GC *Eurocrypt'17*); Masayuki Abe (Director 2015-2017); Josh Benaloh (Director 2015-2017); Anna Lysyanskaya (Director 2016-2018); Bart Preneel (Director 2017-2019, *FSE* Steering Committee); Phillip Rogaway (Director 2016-2018); Francois-Xavier Standaert (Director 2017-2019, *CHES* Steering Committee); Moti Yung (Director 2015-2017, *PKC* Steering Committee).

Attendees (Appointed). Orr Dunkelman (*Eurocrypt'18* General Chair 2017-2018); Steven Myers (*Crypto'17* General Chair 2016-2017) ; Tal Rabin (*Crypto'18* General Chair 2017-2018); Douglas Stebila (Membership Secretary 2017-2020).

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

Absentees (Elected). Brian LaMacchia (Treasurer 2017-2019); Shai Halevi (Director 2017-2019, *TCC* Steering Committee).

Absentees (Appointed). Kenny Paterson (Journal of Cryptology Editor-in-Chief 2017–2019); Josef Pieprzyk (GC *Asiacrypt'18*); Mike Rosulek (Communications Secretary); S.M. Yiu (GC *Asiacrypt'17*).

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

1.3. **Minutes.** The *Eurocrypt'17* Board meeting minutes have already been approved and published online. Cachin thanks Preneel and Bos for finishing the minutes in a timely manner.

1.4. **Action Points.** Cachin briefly reviews the status of action items identified from the *Eurocrypt'17* meeting.

- Rogaway: Assist Dodis with a concrete proposal for a scheme for Test of Time awards. This is ongoing work and a first proposal is finished (see Section 5.2).
- Cachin, Paterson: Clarify the scope of the Journal regarding surveys and Systematization of Knowledge (SoK) papers. This is ongoing, see the new task below.
- Cachin, Steering Committee Representatives: Encourage area conferences to establish processes for video recordings. This is still open and and a new task is created (see below).
- Rogaway: Liaise with *Eurocrypt'18* program co-chairs w.r.t. video recording. This has been done.
- Cachin, Franklin, Paterson: Sort out what to do with the "old" Journal of Cryptology submissions. This is ongoing work, there is progress but more work needed. See new task in Section 2.2.
- Steering Committee representatives: Encourage area conferences to have their websites hosted on the IACR server. This task has been completed. All events except TCC use the new format. Cachin thanks the web team efforts of McCurley, Rosulek, and Yu.

- Stebila: Propose a Privacy Policy for the IACR website. This has been done. Cachin thanks Stebila for all his work here.
- LaMacchia, Rosulek, Stebila: Consider the implications of life-time membership. This has been done. The life-time membership is not considered (see the report for full details).
- LaMacchia,Cachin,Stebila: Renegotiate the UCSB contract with IACR. This is still open, see new task below.
- Bos: Update list of committees in the svn. This has been done.
- Rogaway: Write up an IACR Conflict of Interest Policy and submit it for approval to the President for further discussion and review by the Board. This has been done. See Section 5.1.
- Rogaway: Collect reports from program chairs of conferences of last 2 years and ask them about the work load in this model. This is still open, see the new task below.
- LaMacchia, Abdalla, Myers: Review the GC guidelines and in particular the financial aspects. This is still open, see the new task below.
- Rabin: Update the general chair guidelines on the font size for badges. This has been done. Cachin thanks Rabin for her work.
- Cachin: Coordinate the updates of GC and PC guidelines. This is ongoing work, see the new task below.
- 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 is still open, see new task below.
- Preneel: Update the PC guidelines to include the ToSC hybrid model and the relationship between Transactions on Symmetric Cryptology and Journal of Cryptology. This is still ongoing work, see new task below.
- Cachin, LaMacchia, Rose, Bos: Negotiate with the Real World Cryptography on the sponsoring by IACR. This has been done.
- Cachin, LaMacchia: Identify suitable candidate for sponsorship coordinator. This is still open, see new task below.
- Cachin: Check status of *Asiacrypt'17* and *Asiacrypt'18*. This has been done (but see new task in Section 10.1).
- Dunkelman: Revise the proposed statement and submit it for Board approval. The work on the standards statement is still ongoing, see the new task below.

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

Action Point **2: Cachin, Steering Committee Representatives** *(no time set)*:
Encourage area conferences to establish processes for video recordings.

Action Point **3: LaMacchia, Cachin, Stebila** *(no time set)*:
Renegotiate the UCSB contract with IACR.

Action Point **4: 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 **5: LaMacchia, Abdalla, Myers** *(no time set)*:
Review the GC guidelines and in particular the financial aspects.

Action Point **6: Cachin** *(no time set)*:
Coordinate the updates of GC and PC guidelines.

Action Point **7: Benaloh, Orman** *(no time set)*:
Clarify in the PC Guidelines the role of the Archive and how chairs can facilitate (in particular in relation to front matter).

Action Point **8: Preneel** *(no time set)*:
Update the PC guidelines to include the ToSC hybrid model and the relationship between Transactions on Symmetric Cryptology and Journal of Cryptology.

Action Point **9: Cachin, LaMacchia** *(no time set)*:
Identify suitable candidates for sponsorship coordinator.

Action Point **10: Dunkelman** *(no time set)*:
Revise the proposed standards statement and submit it for Board approval.

1.5. ***Crypto'17* and solar eclipse status.** Myers gives a brief overview of the status of *Crypto'17*. He highlights there is a large number of registered attendees: there are over 420 registrations which is 15 to 20 percent more compared to other Crypto events. This is a good result for a Crypto which is not co-located with CHES. *Crypto'17* uses the new website and registration system and this worked without any problems. Cachin thanks Stebila for all his hard work done to make this happen. Monday there is a different coffee break in order for attendees to watch the eclipse, glasses are part of the welcome package. The 30th IEEE Computer Security Foundations Symposium (CSF) is co-located with *Crypto'17*. The coffee breaks are together as well as the invited talk. There are six registrations for both CSF and *Crypto'17*. Due to sponsoring and the NSF grant we were able to hand out travel grants for student housing + waived registration. The distinguished lecture by Goldwasser is being postponed and is replaced by an invited talk by John Martinis titled "Prospects for a Quantum Factoring Machine" due to last-minute unforeseen circumstances. Cachin thanks Meyers for all his hard work.

2. Officer and Appointee Reports

2.1. **Treasurer.** Benaloh presents some of the details mentioned in the written report by LaMacchia. Benaloh explains some of the changes in more detail: notably, due to this effort the credit card transaction fee has been reduced which saves around 30k$ per year. Cachin thanks LaMacchia for his continued efforts to reduce the overhead for the IACR.

2.2. **JoC Editor in Chief.** Cachin gives an overview of the current status of the Journal of Cryptology (JoC). Best papers are invited to JoC, one of the motivations is the that JoC is ISI indexed. There are still a number of "old" (pre-electronic) papers in the backlog of JoC even after the initial work to try and clean this up. It is unclear how the JoC and the new Transactions should handle best papers.

> Action Point **11: Cachin, Paterson** *(no time set)*:
> Sort out what to do with the pre-electronic Journal of Cryptology submissions.

> Action Point **12: Cachin, Paterson** *(no time set)*:
> Sort out how to handle best papers for ToSC and TCHES in relationship with the JoC.

2.3. **Program chair contact.** No update.

2.4. **Communications Secretary.** A report has been circulated and Cachin gives an overview of the work done on behalf of Rosulek. Currently, https is used everywhere online for the IACR together with the improvements to the IACR webpages. Cachin thanks Rosulek and Yu in absentia for the continued work.

> Action Point **13: Rosulek** *(Dec 31 2017)*:
> Finish the work on the news alert system.

2.5. **Membership Secretary.** Stebila (Membership Secretary) gives a presentation about the current status. He outlines the work done on the new registration system and the fact that IACR will soon accept Bitcoin as payment. There follows a discussion about the option of having a European bank account for the IACR since transferring (and converting) money back and forth from US Dollars to Euros incurs a significant overhead. The conclusion is that an European bank account is currently not an option due to the additional tax work involved. Cachin thanks Stebila for his continued work.

> Action Point **14: Stebila** *(no time set)*:
> Update the General Chair guidelines for the new registration system.

2.6. **Archivist.** No update.

3. Program Chair and other appointments

3.1. **Program and General Chair List Maintenance.** Cachin quickly explains the procedure and the role of the various lists and calls for suggestions for new names. Lai points out that the Asiacrypt Steering Committee has a list of potential program chair names and this will be shared.

> Action Point **15: Lai** *(no time set)*:
> Share the list used by the Asiacrypt Steering Committee for potential program chair names with Bos.

> Action Point **16: Bos** *(no time set)*:
> Update the Program and General Chair List.

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

Decision 1. *Yuval Ishai is appointed Program Chair (rolling co-chair for Eurocrypt'19 and Eurocrypt'20. [Ishai subsequently accepted.]*

3.3. **IACR Distinguished Lecturer 2019 (at Eurocrypt).** 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 2. *Cynthia Dwork is invited to deliver the Distinguished Lecture at Eurocrypt'19. [Dwork subsequently accepted.]*

4. Internal Committee appointments, reports, and decisions

4.1. **Fellows Committee, info.** Cachin points out that the Fellows Committee still should check that all information online is up to date.

> Action Point **17: Lysyanskaya, Rosulek** *(no time set)*:
> Check and ensure all information online is up to date.

4.2. **Audit Committee, report.** The Audit Committee did not meet yet.

> Action Point **18: Cachin** *(no time set)*:
> Kick-off the process for the Audit Committee.

4.3. **Endowment Committee, Report.** Rose mentions that the Endowment Committee will meet this Wednesday during Crypto.

> Action Point **19: Rose, LaMacchia** *(no time set)*:
> Resume the meetings between the Endowment Committee and the Treasurer.

4.4. **Election Committee.** The election Committee consists of Abdalla, Preneel, and Rabin (chair). The role of the Committee is discussed and the members of the Board are asked to encourage members of our community to run for the three open Director positions. Cachin asks if the nomination forms are available online and this is confirmed by the chair of the committee.

4.5. **Ethics Committee.** The Ethics Committee has received one incident which it has dealt with.

4.6. **Schools Committee.** The committee received four proposals for this round. Due to the involvement of Svetla Petkova-Nikova (member of the Schools Committee) Yung acted as a proxy for this proposal.

Abdalla explains the four proposals in more detail. One of the proposals did not meet the requirements since it already takes place coming September but is still considered. Cachin proposes to vote on the different proposals but since the Board members did not receive the four proposals before this meeting it is decided that this vote takes place electronically in two weeks time.

> Action Point **20: Cachin** *(no time set)*:
> Organize the vote related to the four school proposals.

There follows a discussion what kind of schools the IACR should fund. Benaloh expresses his view that schools that are sponsored need to cover new topics. Cachin explains this funding is not intended for recurring schools. This might penalize people who do more work by organizing such schools on a regular interval as pointed out by Dunkelman.

5. Procedures, bylaws and Guidelines

5.1. **Conflict policy for program Committees.** Rogaway present the proposal by Cachin and himself for a new Conflict of Interest (CoI) policy. This proposal is in general received positively but there are some concerns. There is a discussion what happens if a paper is rejected or accepted and it turns out there was a CoI, it is pointed out that this should then be reported to the Ethics Committee.

There is a discussion related to (dis)allow conflicted reviews as mentioned in the current proposal. The motivation for such conflicted reviews is that it might give additional expert opinion. Dunkelman suggests to only keep such reviews in the comments section and not provide to the authors of the paper. Rose is against such "tainted evidence" and this is backed up by a majority of the Board.

Decision 3. *The Board decides to remove the possibility for a conflicted review in the CoI policy.*

Lysyanskaya would like to see a more enforceable CoI with fewer rules, people need to be more ethical. Cachin points out that this is what we currently have and we received too many complaints and this is not working. Bos suggests to change the wording for CoI for companies: use independent part of companies instead of locations. Rabin suggests to highlight in the abstract text that people should use their common sense. Abe asks what to do with internship students and how they are covered in this CoI. The Board discusses the various options when co-authors are in conflict.

Decision 4. *The Board decides that the CoI policy marks co-authors in conflict if they have at least two papers published together in the last three years.*

The text for the CoI policy will be finalized by a Committee soon after the meeting.

> Action Point **21: Preneel, Cachin, Rabin, Rose, Rogaway** *(no time set)*:
> Continue the effort for a CoI policy and create a new proposal using the decisions made during the BoD meeting.

5.2. **Test-of-time awards.** Cachin presents the current work done on the proposal for a test-of-time award. He explains this is also used in other communities and complements the best paper awards. The current proposal uses the citation count as the main metric. There is a discussion if this metric is the best way to proceed. Cachin asks if the Board should continue to work on such an award.

Decision 5. *The Board decides to continue to work out a proposal for the Test of Time award.*

> Action Point **22: Rabin (chair),Dunkelman,Standaert,Yung,Cachin** *(November)*:
> Work out a new proposal for a Test of Time award.

5.3. **Carbon-neutral conferences, discussion.** Standaert presents his proposal with as goal achieving net zero carbon emissions by balancing a measured amount of carbon released with an equivalent amount sequestered or offset, or buying enough carbon credits to make up the difference. The Board agrees this is an important topic but Myers wonders how this would look like in practice. Cachin points out that co-location and the video recordings of the presentations is already a first step in the right direction. Benaloh suggests to make the total carbon cost per conference visible on the webpage. Rogaway points out that NSF grants can be used to compensate for carbon neutral travel. Cachin proposes to have an additional virtual Board meeting in December and Dunkelman suggests to put information related to carbon compensation on the *Eurocrypt'18* webpage.

> Action Point **23: Cachin** *(no time set)*:
> Set up a Doodle to determine the best time to have a virtual meeting this December.

> Action Point **24: Dunkelman** *(no time set)*:
> Put information related to carbon neutrality on the *Eurocrypt'18* webpage.

5.4. **Term limits for Board positions, open discussion.** This topic is put on the agenda by Rabin. She proposes that one can only have the same position twice. There is a brief discussion if this proposal makes a distinguish between a Director or Officer position. It is pointed out that there is no precedent where a member of the Board has served more than twice in the same Officer role. Cachin calls for a vote on this topic.

Decision 6. *The Board decides to not investigate term limits for the Board positions.*

5.5. **Update of General-Chair guidelines.** This is ongoing work by the President. There is no time to discuss this topic.

5.6. **Update of Program-Chair guidelines.** This is ongoing work by Preneel. There is no time to discuss this topic.

5.7. **Appointing Program Chairs.** This additional item has been put on the agenda by Rabin. Rabin asks for a revision of the bylaws to change Article VIII which currently states that for the General Conferences the Program Chair is appointed by the Officers and Elected Directors of the Board while for the Area Conferences the respective Steering Committee selects a Program Chair and submits this to the Board for approval. Rabin suggests that the Board should appoint the Program Chair, just like any other decision of the Board.

Decision 7. *The Board decides not to change the Bylaws (Section VIII).*

5.8. **Diversity, discussion.** This topic has been removed from the agenda by Rabin since no preparations were made. The Board decides to put this on the agenda for the next meeting.

6. Conferences

6.1. **Affiliated workshops at conferences, esp. Crypto '18.** Cachin highlights and encourages more affiliated workshops with our flagship conferences. Eurocrypt had 100 additional attendees due to affiliated workshops. Moreover, this also has a positive impact on becoming more carbon-neutral. Stebila points out that such affiliated events have an impact on the registration system, so if such events take place he must be informed in time.

> Action Point **25: Dunkelman, Stebila** *(no time set)*:
> Align and work out any potential issues with respect to the registration for *Eurocrypt'18*.

> Action Point **26: Dunkelman** *(no time set)*:
> Work out a Call for Affiliated Workshops for *Eurocrypt'18*.

> Action Point **27: Rabin, Cachin** *(no time set)*:
> Work out a Call for Affiliated Workshops for *Crypto'18*.

6.2. **Visa.** This additional item was but on the agenda by Rose. Rose raises the issue with respect to visa and asks how many were denied for *Crypto'17*. Meyers explains that he is aware of two denied visa applications but this might be more due to visas which are delayed.

7. Publications

7.1. **ToSC status.** Preneel explains that everything is going smoothly for ToSC. There are around 10 to 12 accepted papers per round which has the effect that FSE is extended by half a day to 3.5 days.

7.2. **TCHES status.** Cachin explains that Springer has been notified about the discontinuation of the publication of the CHES proceedings in LNCS as of the 2018 edition. The preperations of TCHES are underway as expected.

7.3. **ISI/Springer.** This additional item has been put on the agenda by Preneel. Preneel explains that a substantial part of IACR LNCS publications of the last years have not been indexed by Thomson-ISI. This has had a negative impact on the Impact Factor of the Journal of Cryptology and it may be a problem for the future Impact Factor of the IACR Transactions. Springer claims that they have submitted the necessary meta data to Thomson-ISI as required by the publication contract.

> Action Point **28: Cachin, Preneel** *(no time set)*:
> Contact Springer to clarify which conferences are being considered for ISI indexing.

8. Conference reports since last BoD Meeting (information)

8.1. **Eurocrypt '17 summary.** Abdalla gives a brief summary of *Eurocrypt'17*, they had 491 attendees. The financial summary will be ready soon.

> Action Point **29: Abdalla** *(no time set)*:
> Complete the financial summary and provide this to the treasurer.

9. Forthcoming conferences (information)

9.1. **Asiacrypt '17.** See later.

9.2. **Eurocrypt '18.** Dunkelman explains that the venue contract will be signed very soon. No time to discuss this further.

9.3. **Crypto '18 with NIST workshop on post-quantum.** No time.

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

10.1. **Asiacrypt Steering Committee (information).** Cachin explains the current situation with *Asiacrypt'17*. The President was informed a couple of weeks back that the venue was last minute not available. The impact on the budget and registration fees is being investigated and a new budget needs to be worked out. More information soon.

The dates for *Asiacrypt'19* have changed to resolve a conflict with the Thanksgiving holiday. *Asiacrypt'19* will take place from December 8 to 12 in Kobe (Japan).

> Action Point **30: Cachin** *(no time set)*:
> Clarify venue status *Asiacrypt'17*.

> Action Point **31: Cachin** *(no time set)*:
> Clarify status *Asiacrypt'18*.

10.2. **Crypto '19 general chair appointment.** Several excellent candidates are nominated, and after discussion a candidate is selected.

Decision 8. *Muthu Venkitasubramaniam is appointed General Chair for Crypto'19, late Aug, UCSB, Santa Barbara. [Venkitasubramaniam subsequently accepted.]*

10.3. **CHES Steering Committee (information).** Update will follow after CHES takes place in September.

> Action Point **32: Standaert** *(December)*:
> Provide an update from the CHES Steering Committee.

10.4. **FSE Steering Committee (information).** The *FSE'19* proposal (which is in the repository) is discussed.

Decision 9. *The proposal for FSE'19 in Paris is approved with Jérémy Jean as General Chair and Florian Mendel and Yu Sasaki as Program Chairs.*

> Action Point **33: Preneel** *(no time set)*:
> Provide Cachin and LaMacchia with an updated budget.

10.5. **PKC Steering Committee (information).** No time.

10.6. **TCC Steering Committee (Information).** Nothing.

10.7. **Schools Committee (info, past and scheduled schools).** No time, this will be done per e-mail.

11. Closing Matters

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

- The Conflict of Interest policy discussions.
- The test-of-time awards discussion.

11.2. **Review of Action Points.** Cachin asks Bos to summarize the action points. After this summary the meeting closes at 18:36.

12. Intermediate Board Decisions

Decision 10 (2016/09/20)**.** *The Board approves the CHES'18 proposal, meaning that CHES'18 will be held in Amsterdam (Netherlands) with Ileana Buhan and Peter Schwabe as General Chairs, and Daniel Page and Matthieu Rivain as Program Chairs.*

Decision 11 (2017/01/29)**.** *The Board approves Halevi's call for posting a response to Trump's travel ban.*

Decision 12 (2017/03/09)**.** *The Board approves the PKC'18 proposal, meaning that PKC'18 will be held in Rio De Janeiro (Brazil) with Ricardo Dahab as General Chair and Michel Abdalla as Program Chair.*

Decision 13 (2017/03/09)**.** *The Board approves the minutes the Board meeting held at Crypto'16.*

Decision 14 (2017/03/09)**.** *The Board approves the proposal by the Treasurer to open a new bank account at 1st Security Bank, Seattle.*

Decision 15 (2017/07/11)**.** *The Board approves of the new guidelines for the Real World Cryptography Symposium.*

Decision 16 (2017-7)**.** *The Board approves the budget for the Real World Cryptography Symposium in Zurich (Switzerland).*

Decision 17 (2017-8)**.** *The Board approves the minutes of the Board meeting held at Eurocrypt'17.*