# MINUTES IACR BOARD MEETING *EUROCRYPT'17*

PARIS, FRANCE, 30 APRIL 2017

## 1. Opening Matters

1.1. **Welcome, roll of attendees, identification of proxies.** At 10:08 Cachin opens the meeting and he briefly goes around for an introductory round, confirming attendees and establishing who is holding proxies. Myers arrived at 10:19. Abdalla left the meeting at 17:20. Paterson attended the meeting for part of the afternoon.

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 Standaert on carbon neutrality was added to other matters. There was an adjournment for lunch around 13:20.

1.2.1. *Roll of Attendees.* There are 14 full time attendees with LaMacchia holding proxy for Rose, Preneel for Bos, Rabin for Halevi and Lysyanskaya, and Myers for Rosulek. Rabin also held a proxy for Abdalla for the last part of the meeting.

*Attendees* (Elected). Michel Abdalla (Director –2018, GC *Eurocrypt 2017*); Masayuki Abe (Director –2017); Josh Benaloh (Director –2017); Christian Cachin (President –2019); Brian LaMacchia (Treasurer –2019); Bart Preneel (Director –2019, *FSE* Steering Committee, acting Secretary for this meeting); Phillip Rogaway (Director –2018); François-Xavier Standaert (Director –2019, *CHES* Steering Committee); Moti Yung (Director –2017).

*Attendees* (Appointed). Orr Dunkelman (GC *Eurocrypt'18*); Steve Myers (GC *Crypto'17*); Kenny Paterson (Journal Editor-in-Chief –2016) (partial attendance); Tal Rabin (GC *Crypto'18*); Douglas Stebila (Membership Secretary –2020).

*Attendees* (Representatives and Others). Yu Yu (Webmaster).

*Absentees* (Elected). Joppe Bos (Secretary –2019); Shai Halevi (Director –2019, *TCC Steering Committee*). Anna Lysyanskaya (Director –2018); Greg Rose (Vice-President –2019);

*Absentees* (Appointed). Josef Pieprzyk (GC *Asiacrypt'18*); Mike Rosulek (Communications Secretary); S.M. Yiu (GC *Asiacrypt'17*);

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

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

1.4. **Review of Open Action Points.** Cachin briefly reviews the status of action items identified from the *Crypto'16* meeting.

(1) Test of Time award. Deferred to July 1st (see new action item below).
(2) PR operation: no action was taken since no volunteer has been found.
(3) Make membership and attendee information available to members and attendees. This has been done.
(4) Sponsorship. Replaced by action items related to the RWC discussion.
(5) Relation ToSC-JoC. A solution has been developed. See also Section 2.2.
(6) Scope JoC. This was not discussed due to the absence of Paterson. Action item has been deferred to July 1st.
(7) Closed. General conferences should host their website on the new IACR server.
(8) Front matter in archive. Changed into new action item in Agenda item 5.
(9) Align categories from budget and report. Changed into new action item in Agenda item 5.
(10) GC/PC guideline revision. Changed into several new action items in Agenda item 5.
(11) Video recording is now mentioned in the call for papers for conferences. New action item for steering committee representatives and Cachin to follow up with steering committees.
(12) ToSC contract and publication. This has been done.

Action Point **1: Rogaway** *(July 1st)*:
Assist Dodis with a concrete proposal for a scheme for Test of Time awards.

Action Point **2: Cachin, Paterson** *(July 1st)*:
Clarify the scope of the *Journal* regarding surveys and Systematization of Knowledge (SoK) papers.

Action Point **3: Cachin, Steering Committee Representatives** *(July 1st)*:
Encourage area conferences to establish processes for video recordings.

Action Point **4: Rogaway** *(July 1st)*:
Liaise with EC'18 program co-chairs w.r.t. video recording.

1.5. ***Eurocrypt'17* Status.** Abdalla (GC *E'16*) gives a brief presentation on the status of *Eurocrypt'17*. There are 480 registered attendees for Eurocrypt (the largest Eurocrypt ever); 320 people are registered for each day of the pre-conference workshops on Saturday and Sunday. The number of student attendees is about 180. Registrations came in later than expected. The central location, the co-location with European Security & Privacy and the workshops may have helped. Managing conference and workshop together is a challenge, in particular in terms of budget; there was some help from European Security & Privacy. The conference is expected to have a small loss. Dealing with special meals is challenging.

Cachin thanks Abdalla for his hard work, including his extensive coordination with the workshops.

## 2. Officer and Appointee Reports

2.1. **Treasurer.** LaMacchia reports that the transition from Rose has been completed. He presents a detailed financial report. He reports that IACR is financially stable, explaining some of the details mentioned in his written report. Credit cards costs are high; substantial savings are possible by changing the processor. He proposes a budget for 2017 and plans to propose a budget for 2018 before *Crypto'17*. He recommends to keep the membership fee at 50$/25$. A tax address has been established in Seattle.

Cachin thanks LaMacchia for his hard work.

2.2. **JoC Editor in Chief.** Paterson summarize his written report. He describes the hand-over from Ivan Damgård that includes all the ongoing submissions including 60 pre-electronic submissions (pre-January 2014). The electronic system has 68 papers under review, including 5 from 2014, 19 from 2015 and 26 from 2016. There are 42 submissions since January 1, 2017 of which 27 have been rejected so far and 15 are under review. The review delays are clearly too high which negatively affects the reputation of the journal. Paterson proposes to aim for a 1-year reviewing period (first round) for the papers submitted from January 2018 onwards. JoC continues to invite best papers from the conferences; they can still be rejected. At least 25% material should be new compared to conference versions, which may be a concern since some conference papers are already quite long (30 pages). The publication backlog is currently 1 year but there is an online first mechanism. A special issue has been planned on TLSv1.3 with Colin Boyd as guest editor. The Editorial Board is discussing other ideas for special issues. The online system for editors is quite non-intuitive and some changes are being made to improve this.

Preneel asked whether there are statistics on rejections of invited papers from the conferences. Paterson answers that he does not have these statistics.

Abdalla suggests to introduce a hard 3-month revision deadline for the authors. Paterson states that this is the current policy but that he can give extensions.

Preneel suggests to mandate that all authors of old papers submit to the new electronic system.

Action Point **5: Cachin, Franklin, Paterson** *(1 July)*:
Sort out what to do with the "old" Journal of Cryptology submissions.

The relationship between Transactions on Symmetric Cryptology (ToSC) and Journal of Cryptology (JoC) is discussed. Currently the best ToSC papers are invited to be submitted to Journal of Cryptology but as ToSC is a conference-journal hybrid this process should be different from that of conferences.

**Decision 1** (approved unanimously)**.** *The Board proposes that the ToSC co-editors select per round an average of approximately one paper for submission to JoC; the paper is forwarded together with the reviews and the JoC editor-in-chief processes these papers in a fast-track procedure. There will be careful coordination so that rejection from JoC still would allow timely publication in ToSC.*

The program chair guidelines will be updated to reflect this change.

Cachin thanks Paterson for his hard work.

2.3. **Program chair contact.** There are no major issues to report. One ethics issue has come up and will be handled by the ethics committee. Some program chair reports are still missing. Benaloh announces that he wants to step down in this role.

The Board unanimously appoints Rogaway as program chair contact.

2.4. **Communications Secretary.** There is a new website template for IACR conferences. This template is mobile-device friendly. From AC'17 onwards general conferences will be hosted on the IACR server. Area conferences are strongly encouraged to also run their websites on the IACR server.

Cachin thanks the communications team for their effort.

Rabin points out that the font on the badges is sometimes too small; she will update the guidelines (see Action Point 14).

> Action Point **6: Steering committee representatives** *(July 1st)*:
> Encourage area conferences to have their websites hosted on the IACR server.

2.5. **Membership Secretary.** Stebila presents an update on the membership composition. He points out that over the last seven year membership has been relatively stable, with a slightly increased percentage of students. We have 5 senior members for 2018. We expect a substantial growth of membership when Real World Crypto will be sponsored by the IACR.

Stebila is working on the IACR privacy policy. The final version will be submitted to the IACR Board for approval.

The conference registration system is being rewritten: more modern code architecture, revised data model (add excursions), modularity of payment processor. A first version has been trialed for *Eurocrypt'17*. Members will have more services on-line. There are some issues related to JoC subscriptions that will be resolved. The role of the UCSB secretariat is diminishing and there are some interface issues w.r.t. UCSB.

Preneel points out that it is useful to keep the address at UCSB.

A board member[1] proposes to consider a one-time fee for life-time membership.

Cachin thanks Stebila for his hard work.

> Action Point **7: Stebila** *(July 1st)*:
> Propose a Privacy Policy for the IACR website.

> Action Point **8: LaMacchia,Rosulek,Stebila** *(July 1st)*:
> Consider the implications of life-time membership.

> Action Point **9: LaMacchia,Cachin,Stebila** *(Crypto'17)*:
> Renegotiate the UCSB contract with IACR.

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

## 3. Program Chair and other appointments

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

3.2. **Crypto '18–'19.** Hovav Shacham has already been appointed as one of the co-chairs for *Crypto'18*. Several excellent candidates are nominated, and after discussion a candidate is selected.

**Decision 2.** *Sasha Boldyreva is appointed Program Chair (rolling co-chair) for Crypto'18 and Crypto'19.*

3.3. **Asiacrypt '18–'19.** Thomas Peyrin has already been appointed as one of the co-chairs for *Asiacrypt'18*. Several excellent candidates are nominated, and after discussion a candidate is selected.

**Decision 3.** *Steven Galbraith is appointed Program Chair (rolling co-chair) for Asiacrypt'18 and Asiacrypt'19.*

## 4. Internal Committee appointments, reports, and decisions

> Action Point **10: Bos** *(1 July)*:
> Update list of committees in the svn.

4.1. **Fellows Committee.** Five fellows have been selected by the fellows committee.

[1] Changed after approval.

4.2. **Audit Committee.** There is some discussion on the difference between a finance and an audit committee and on the terms of reference of the committee. The composition of this committee will be discussed at a later date.

4.3. **Endowment Committee.** The endowment committee met at Crypto'16 but no report was sent. The composition is left unchanged.

4.4. **Election Committee.** The following people are appointed to the 2017 election committee: Abdalla, Rabin, Preneel.

4.5. **Ethics Committee.** The following people are appointed to the ethics committee: Rose (vice-president), Rogaway (program chair contact), Benaloh.

4.6. **Schools Committee.** The current composition is: Abdalla, Abe, Lysyanskaya, Boldyreva, Petkova-Nikova. For an update see item 10.6.

## 5. Procedures, Bylaws and Guidelines

5.1. **Conflict of interest policy for program committees.** Rogaway point out the extensive scientific literature on bias in peer reviewing. He analyzed the Conflict Of Interest (COI) policies of our past conferences and the IACR guidelines for program chairs and reviewers. Several are too weak and the guidelines are rather vague. He has analyzed the COI policies of several major security events. Based on this he has drafted a proposal together with Mihir Bellare.

Rabin expressed strong reservations against a formal IACR COI policy as this would infringe on the autonomy of program chairs. She also expressed strong reservations against the first condition mentioned below (published joint work in the prior two years): 1) this would create the risk that the experts in the area of the paper who are best qualified would not be able to review a paper or to act as 'champion' for a paper in the program committee; 2) prolific authors would have COIs with a large number of papers and would not be able to participate effectively in a program committee. Rogaway commented that experts in an area are indeed the best qualified to judge the technical contribution itself, but they may perhaps be too close to the work to evaluate its importance.

The Board first voted on the decision to establish a formal Conflict Of Interest policy for IACR. This decision was approved with 3 votes against.

Subsequently the IACR Board requested Rogaway to write up an IACR Conflict of Interest Policy based on the following principles:

> A reviewer has an automatic conflict of interest (COI) if an author if they
> (1) published joint work in the prior two years,
> (2) were author's primary doctoral thesis advisor and advisee, no matter how long ago,
> (3) shared an institutional affiliation within the last year, or
> (4) are in the same family.
>
> During the submission process, authors will be asked to identify all members of the program committee with whom they have an automatic COI. Authors may separately explain other potential COIs (such as close friendships, personal animosities, or reviewers with competing research results). The program chairs will decide if a potential COI should be treated as a COI. It is the responsibility of all authors of a paper to ensure the accuracy of all provided COI information. Papers with incorrect or incomplete automatic COI information are subject to immediate rejection.
>
> When a program committee member has a COI with a paper, they may not see the paper or its reviews, comment on it, or vote for it for any awards.
>
> A subreviewer may not review a paper known by them to have an author with whom they have a COI.

The decision was approved with 11 votes in favor, 3 against, and 4 abstentions.

Rogaway's proposal for an IACR Conflict of Interest Policy will be further discussed by the Board. Once this IACR Conflict of Interest Policy will have been agreed, there will be further discussion on whether this is made mandatory as a minimum policy.

> Action Point **11: Rogaway** *(1st July)*:
> Write up an IACR Conflict of Interest Policy and submit it for approval to the President for further discussion and review by the Board.

5.2. **Co-chairs at conferences.** There was an extensive discussion on the proposal of Rabin to replace rolling co-chairs (current model for general conferences and ToSC) by parallel co-chairs (current model for CHES).

> Action Point **12: Rogaway** *(July 1st)*:
> Collect reports from program chairs of conferences of last 2 years and ask them about the work load in this model.

5.3. **Diversity.** Due to lack of time this item will be dealt with at a later date.

5.4. **Update of General Chair Guidelines.** Updates are needed to General Chair Guidelines to reflect changes in practices and policies.

> Action Point **13: LaMacchia,Abdalla, LaMacchia,Myers** *(July 1st)*:
> Review the GC guidelines and in particular the financial aspects.

> Action Point **14: Rabin** *(July 1st)*:
> Update the general chair guidelines on the font size for badges.

> Action Point **15: Cachin** *(July 15th)*:
> Coordinate the updates of GC and PC guidelines.

5.5. **Update of Program Chair Guidelines.** Updates are needed to Program Chair Guidelines to reflect changes in practices and policies.

> Action Point **16: Benaloh, Orman** *(July 1st)*:
> Clarify in the PC Guidelines the role of the Archive and how chairs can facilitate (in particular in relation to front matter).

> Action Point **17: Preneel** *(July 1st)*:
> Update the PC guidelines to include the ToSC hybrid model and the relationship between Transactions on Symmetric Cryptology and Journal of Cryptology.

## 6. Conferences

6.1. **Proposal for IACR Real-World Cryptography symposium.** The proposal from Real-World Cryptography to become an IACR-sponsored event is discussed. There was an extensive discussion on how to deal with reserves and sponsoring and how to protect the specific nature of Real-World Cryptography.

The IACR Board unanimously approves the following decision:

**Decision 4.** *The Real World Cryptography (RWC) conference becomes an IACR sponsored event along the lines of the proposal of the RWC steering committee with some financial independence within bounds to be negotiated by the IACR Officers.*

> Action Point **18: Cachin,LaMacchia,Rose,Bos** *(August 1st)*:
> Negotiate with the Real World Cryptography on the sponsoring by IACR.

The IACR Board will search for a sponsorship coordinator as a non-voting Board member.

> Action Point **19: Cachin,LaMacchia** *(August 1st)*:
> Identify suitable candidate for sponsorship coordinator.

6.2. **Affiliated workshops at conferences.** Several workshops were organized on the Saturday and Sunday before Eurocrypt together with European Security & Privacy. This was a great success: a call was published for affiliated events and 18 workshops were selected. There are 320 attendees each day, of this 180 are registered for both days. The practical organization created a substantial overhead, so it would be best to appoint a member of the organizing team to coordinate the workshops. Affiliated events are supported by the registration system. As the registration fee is low, it was decided to not include IACR membership for these workshops. The IACR Board wants to strongly encourage general chairs of general conferences to organize workshops around the conference.

Cachin thanks Abdalla for this efforts in organizing these workshops.

## 7. Publications

7.1. **Springer Contract.** A new 2-year contract with Springer has been signed. Each event receives a financial contribution per book volume extra rather than free paper proceedings copies. The Springer representatives will pay registration fees.

7.2. **ToSC report.** Preneel gave an update on the progress of Transactions of Symmetric Cryptology. He explained the conference/journal hybrid publication model and the lessons learned. All papers are published in gold open access in electronic format. The review process combines the best of journal and conference reviewing. More papers have been accepted, so in the future the event may be extended by 0.5 or 1 day. The experience is very successful. Three issues of ToSC have been published.

7.3. **Relationship between ToSC, eprint, JoC.** Currently final versions to ToSC are submitted automatically to eprint by the webreview software. It is not clear that this makes sense in view of the gold open access. Nevertheless, some authors prefer to have their papers also on eprint; they are of course free to submit their paper to eprint; this may increase visibility but but may result in citation to the eprint version; authors could indicate in a footnote "cite as" to reduce this problem.

7.4. **Proposal for ToCHES.** A proposal from the CHES Steering Committee to switch from a conference model to hybrid conference/journal model was submitted. The proposal is very similar to that of ToSC; one difference is that there are 2 parallel co-editors in chief per year (no rolling chairs). There was some discussion on the name.

**Decision 5** (unanimous)**.** *The proposal from the CHES Steering Committee to switch to the hybrid conference/journal model for CHES is accepted.*

## 8. Conference reports since last BoD Meeting

8.1. ***Asiacrypt'16*.** LaMacchia reports that the conference broke even.

8.2. ***Crypto'16*.** LaMacchia points out that a detailed report is available in the svn.

## 9. Forthcoming Conferences

9.1. ***Crypto'17*.** Crypto'17 will be held at UCSB from August 20-24. Myers (GC *Crypto'17*) informs the Board that everything is on track including sponsorship. For NSF there is a procedure with more overhead but also more money. There are some concerns w.r.t. lower attendance.

9.2. ***Asiacrypt'17*.** No update is available. The website is online.

| Action Point **20: Cachin** *(June 1)*:<br>Check status of Asiacrypt'17 and '18. |
|---|

9.3. ***Eurocrypt'18*.** Eurocrypt'18 will be held in Tel Aviv on April 29- May 3. Dunkelman (GC *Eurocrypt'18*) informs the Board that everything is on track. There is an issue related to VAT that require further attention.

9.4. ***Crypto'18*.** Crypto'18 will be held at UCSB from August 19-23 (tentatively). Rabin reports everything is on track.

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

10.1. **Asiacrypt'19 proposal.** Mitsuru Matsui presents a proposal for Asiacrypt'19 in Kobe, Japan. The proposed general chair is Mitsuru Matsui and the proposed local organizing chair is Yasuyuki Sakai. The proposed venue is the Kobe Portopia Hotel and the dates are November 24-28, 2019. The registration fee is US$600. The budget is based on 250 attendees.

There is some discussion on the dates, that interfere with Thanksgiving that is the most important family holiday in the US; this may create travel problems for US participants. Unfortunately the hotel is not available one week later. The general chair is requested to explore to shift the event one week earlier or one or two weeks later to avoid the Thanksgiving week.

**Decision 6** (unanimous)**.** *The proposal for Asiacrypt 2019 in Kobe, Japan is accepted, with Mitsuru Matsui as General Chair.*

10.2. ***CHES* Steering Committee.** Standaert gives an update on *CHES17* in Taipei, Taiwan. There are 130 submissions. The sponsorship budget is 50K$.

10.3. ***FSE* Steering Committee.** Preneel reports that *FSE'17* in Tokyo was very well organized. The conference made a small surplus and a report is in the svn. One point of attention is a scam to impersonate the general chair team in order to sell hotel bookings. Everything is on track with the preparations for FSE'18 in Bruges (March 5-7).

10.4. ***PKC* Steering Committee.** Yung reports on PKC in Amsterdam. The 2018 edition will be held in Brazil but there is no formal approval yet.

10.5. ***TCC* Steering Committee.** A proposal for *TCC 2017* in Goa (India) has been circulated. Proposed general chairs are Shweta Agrawal and Manoj Prabhakaran. Proposed program chairs are Amos Beimel and Stefan Dziembowski. There are some comments on the budget (that uses an outdated template) and on the registration fees.

**Decision 7** (unanimous)**.** *The proposal for TCC 2017 in Goa is approved, with Shweta Agrawal and Manoj Prabhakaran as General Chairs and Amos Beimel and Stefan Dziembowski as Program Chairs.*

10.6. **Schools Committee (Cryptology Schools).** The schools committee did not receive any fundable proposals in the past round. Perhaps more effort should be spent on encouraging submissions. The next deadlines are 30 June 2017 and 31 December 2017. The 2017 budget is 35K$, while individual proposals can receive 5K$-10K$.

## 11. Other Matters

11.1. **Statement about the subversion of crypto standardization processes.** Two statements proposed by Dunkelman on the lack of quality control for cryptographic standards were discussed. The conclusion was that the first statement needs some further wordsmithing and a title. The second proposal will not be endorsed.

> Action Point **21: Dunkelman** *(May 4)*:
> Revise the proposed statement and submit it for Board approval.

11.2. **Make IACR events more carbon neutral.** Standaert submitted a proposal to make IACR events more carbon neutral by email to the Board on April 27. Due to lack of time this item will be dealt with at a later date.

## 12. Closing Matters

12.1. **Draft Agenda for Membership Meeting.** Due to lack of time, there was no time to identify the main issues to discuss at the membership meeting.

12.2. **Review of Action Points.** After a brief review of action points, Cachin closes the meeting at 19.45.