MINUTES IACR BOARD MEETING *CRYPTO'16*

UCSB, SANTA BARBARA, 14 AUGUST 2016

1. Opening Matters

1.1. **Welcome, roll of attendees, identification of proxies.** At 10:04 Cachin opens the meeting and he briefly goes around for an introductory round, confirming attendees and establishing who is holding proxies.

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 noon.

1.1.1. *Roll of Attendees.* There are 19 attendees, holding no proxies, and an observer joining for shorter stretches.

Attendees (Elected). Masayuki Abe (Director –2017); Michel Abdalla (Director –2018, GC *Eurocrypt 2017*); Josh Benaloh (Director –2017); Christian Cachin (President –2016) Anna Lysyanskaya (Director –2018); David Pointcheval (Director –2016, *PKC* Steering Committee); Bart Preneel (Director –2016, *FSE* Steering Committee); Phillip Rogaway (Director –2018); Greg Rose (Treasurer –2016); Nigel Smart (Vice-President –2016); Martijn Stam (Secretary –2016); Moti Yung (Director –2017).

Attendees (Appointed). Ivan Damgård (Journal Editor-in-Chief –2016); Brian LaMacchia (GC *Crypto'16*); Steve Myers (GC *Crypto'17*); Phan Duong Hieu (GC *Asiacrypt'16*); Krzysztof Pietrzak (GC *Eurocrypt'16*); Mike Rosulek (Communications Secretary); abhi shelat (Membership Secretary –2017).

Attendees (Representatives and Others). Hilarie Orman (Archivist), joined during meeting; Yu Yu (Webmaster).

Absentees (Elected). Christof Paar (Director –2016, *CHES* Steering Committee).

Absentees (Appointed). S.M. Yiu (GC *Asiacrypt'17*).

Absentees (Representatives and Others). Kevin S. McCurley (Database Administrator); Shai Halevi (*TCC* Steering Committee); Xuejia Lai (*Asiacrypt* Steering Committee).

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

1.3. **Minutes.** The *Crypto'15* Board of Director minutes are approved with some redaction for content and a brief discussion regarding the timing of these minutes. The *Crypto'15* Membership minutes, *Eurocrypt'16* Board of Director minutes, *Eurocrypt'16* Membership minutes are approved with some editorial comments.

For the latter, Smart mentions that he has discussed with Dodis regarding how to come up with a concrete proposal for Test of Time awards. Rogaway believes that compared to for instance Fellowship awards, there will not be a need for explicit endorsements.

> Action Point **1: Rogaway** *(no time set)*:
> Assist Dodis with a concrete proposal for a scheme for Test of Time awards.

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

(1) This has been done.
(2) Rose has called a meeting of the Endowment committee this Tuesday afternoon.
(3) Orman has been discussing with McCurley and clarifies that Springer metadata is available and can be transformed if needed. Preneel points out that for *ToSC* Springer will not be involved.
(4) Abdalla has updated the School Guidelines.
(5) A draft copyright policy for *ToSC* has been suggested to the *FSE* Steering Committee. A Creative Commons license currently has the preference, but there is still a discussion about the appropriate footnote for papers to indicate their status. Smart mentions that the IACR is in control here because it publishes *ToSC*.

    Preneel explains a further complication regarding additional material, such as code, but also the presentation slides and for instance video of the presentation.
(6) Smart demonstrates how *ToSC* looks on the website.

(7) Cachin has been in touch with Biham. Fellows will be contacted under embargo and the IACR will announce on a date (so their respective institutions can issue a press releases). A summary of the procedure has been stored in the repository. There is a brief discussion on how other societies publicize their Fellows appointments.

Lysyanskaya suggests we could have a more active PR, for instance by having a freelancer publicist on retainer. There is a brief discussion what this would entail; overall there is support for this idea.

> Action Point **2: Lysyanskaya, Rosulek, Smart** *(no time set)*:
> Instigate a more active PR operation

(8) Rose and the Audit committee will meet this Tuesday afternoon.
(9) The PC/Ethics Guidelines are on the agenda.
(10) Cachin has emailed around a proposed clarification and this was implemented.
(11) A revision of the guidelines is in progress.
(12) Cachin has had some ideas to make a redacted version of the attendee list electronic. After some discussion, there is no consensus yet, especially the complication of publishing e-mail addresses.

> Action Point **3: Cachin, shelat** *(no time set)*:
> Cooperate with the Communications Secretary on how to make the membership and attendee information available to members and attendees.

1.5. ***Crypto'16* Status.** LaMacchia (GC *C'16*) gives a brief presentation of the status of *Crypto'16*. He highlights there is a large number of student registrations and explains how the colocation with *CHES'16* will work. A lot of effort has been put into arranging joint events and providing time for mixing the audiences; the rump session and the invited talk on Wednesday are in the program of both events.

There is a puzzle contest as part of the gift and delegate pack. The conference looks to be on budget, although he does note that there is a significant difference in room rent of the two facilities needed for parallel sessions.

Cachin thanks LaMacchia for his hard work, including his extensive coordination with the *CHES* organization.

2. Officer and Appointee Reports

2.1. **Treasurer.** Rose reports that IACR is financially stable, explaining some of the details mentioned in his written report.

Cachin thanks Rose for his hard work.

2.2. **Treasurer – Sponsorships.** Currently the respective general chairs are responsible for soliciting sponsorship. For some (long-time) sponsors it might be beneficial to set up a more general multi-sponsorship arrangement, centrally by the IACR.

Some sponsors will also ask for data (such as involvement of their employees in the conference, but sometimes more) to help them decide. Smart remarks that sponsorship itself should be treated as a donation, not a payment for data or some other service (as in that case VAT would have to be charged).

Increased continuity from year to year would help to smooth out complications with sponsorship and annual subsidies (e.g. from the NSF). Paterson points out other opportunities (such as prizes) that the IACR is currently missing.

> Action Point **4: Rose, Lysyanskaya, LaMacchia** *(no time set)*:
> Come up with a proposal to assist a more continuous approach to sponsorship.

2.3. **JoC Editor in Chief.** Cachin has not yet received a report from Damgård.

2.4. **Future JoC Editor in Chief.** Paterson clarifies that he will take over from Damgård in January 2017. He is looking forward to improving the system that was brought in for online reviewing. He explains his plans in the long and the medium term. For instance, in the medium term he is hoping for more special issues. Given changes elsewhere (such as the *ToSC*), he would like to form a strategic vision of how the *Journal* will fit in such a future landscape. Preneel remarks that the impact factor has gone down in recent years. Lysyanskaya asks whether Paterson is considering to increase the number of papers per year as well.

> Action Point **5: Paterson, Preneel** *(no time set)*:
> Develop a strategy for the relation between IACR's publications, especially *ToSC* and the *Journal*.

Myers asks whether there is value in actively soliciting surveys of systematization-of-knowledge papers.

> Action Point **6: Cachin, Paterson** *(no time set)*:
> Clarify the scope of the *Journal* regarding surveys and SoK.

2.5. **Program chair reports.** Benaloh has received program chair reports but has not uploaded them yet.

2.6. **Communications Secretary.** There is nothing new to report. Rosulek does bring to the fore some past action items where more work is still possible. For instance, templates for conferences (for the website) would be useful.

> Action Point **7: Rosulek** *(Eurocrypt'17)*:
> Initiate a meeting with Kevin etc. to plan (and where possible execute) further changes to the website and its back-end.

2.7. **Membership Secretary.** shelat presents an update on the membership composition. He points out that over the last seven year it has been relatively stable, with a slightly increased percentage of students.

He points out that the conference registration system is nearing the end of its lifetime and he points out a number of urgent needs. Outsourcing building a new system would be an option (but outsourcing the service itself would not). He would like to keep core database scheme intact (though augment to it). A rough estimate for the work needed would be 50k$.

Decision 1. *The Board authorizes the President spend up to 50k$ on a proposal jointly developed between him and the Membership Secretary on upgrading the conference registration system.*

Smart points out that the lack of professional staff and relying only on volunteer work might hinder the future growth of the IACR.

2.8. **Archivist.** Orman provides a backdrop to the written report. Recently she found out about a few papers of which the final version was missing on WebSubRev. There is some unclarity about what WebSubRev can and cannot do.

> Action Point **8: 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).

Smart believes it worthwhile to reconsider the position of the Archive given various changes in the publication process.

Cachin thanks Orman for her hard work.

3. Program Chair and other appointments

3.1. **Cryptology ePrint Archive.** Cachin has discussed with Boldyreva concerning a successor to Smart to serve as ePrint editor. They have approached Tancrède Lepoint, who is willing.

Decision 2. *Tancréde Lepoint is appointed co-editor to the ePrint archive.*

Given the recent clarification in the guidelines, Cachin wonders whether the Board should make an explicit statement to the membership about the role and power of the ePrint editors.

Preneel points out that editors are humans and from that perspective they might make mistakes and some form of private response should be allowed. However, there is a new type of behavior of public discussion on social media etc. and it is unclear whether and how the IACR should respond.

3.2. **Program and General Chair List Maintenance.** Cachin very quickly explains the procedure. Stam 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.

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

Decision 3. *Vincent Rijmen is appointed Program Chair (rolling co-chair for Eurocrypt'18 and Eurocrypt'19. [Rijmen subsequently accepted.]*

3.4. **Asiacrypt 2018 Distinguished Lecturer.** 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 4. *Matsuru Matsui is invited to deliver the Distinguished Lecture at Asiacrypt'18. [Matsui subsequently accepted.]*

4. Internal Committee appointments, reports, and decisions

4.1. **Fellows Committee.** Cachin points out that the Fellows committee still should double-check with Rosulek and Yu to ensure that all information online is up to date.

4.2. **Audit Committee.** Rose mentions that the Audit committee will meet soon.

4.3. **Endowment Committee.** Rose mentions that the Endowment committee will meet soon.

4.4. **Election Committee.** Cachin points out that the Election committee still need to liaise with the Rosulek and Yu to ensure that all information online is up to date. Smart will serve as Chair and Abdalla as returning officer.

4.5. **Ethics Committee.** The committee has received one incident which it is still contemplating.

4.6. **Schools Committee.** The Committee did not receive any proposals for the current round; they have extended the deadline.

Moti Yung has decided to step down and Anna Lysyanskaya will join the committee.

Abe suggests to extend the target to smaller events such as tutorials that directly precede an event (such as a workshop). He describes his positive experience and points out that even very small amounts of support will help these useful initiatives. Preneel recalls the *CHES* model which has a call for associated tutorials without further support from the IACR needed.

5. Procedures, bylaws and Guidelines

5.1. **Update of Bylaws and GC + PC guidelines after 2016 referendum.** Cachin and Smart explain a number of the reasons why updates are needed.

> Action Point **9: Rose** *(no time set)*:
> Review the financial aspects of the general chair guideline.

> Action Point **10: Smart,Stam,Cachin** *(no time set)*:
> Update the general chair guidelines and program-chair guidelines where necessary.

5.2. **Discussion of needed revisions.** One question is whether presenters should be allowed to opt-out to making their slides and recording of the presentation available. LaMacchia points out that this would imply a change to the process such as the Call for Papers. Pietrzak recalls his experience with video-editing for *Eurocrypt'16*. Cachin prefers to appoint someone to liaise with the General Chairs to ensure a consistent (and less cumbersome) process. Yu is willing to engage.

> Action Point **11: Yu** *(no time set)*:
> Initiate a meeting with Kevin to create a consistent process for making the slides and recording of presentations publicly available.

There is a discussion regarding the pros and cons of mandatory recordings. On the one hand, the IACR should try to make IACR's recording as widely as possible. Some people might not have the confidence to have their presentation made available online. At *Eurocrypt'16* 10 people who opted out, at *Crypto'16* there were 2. If recording becomes obligatory, those who object might still submit elsewhere. For invited talks or a panel there might be a reason to make an exception because what was said should not be attributable.

Decision 5. *By default, all presentations at IACR Area and General Conferences will be recorded and published. The President decides on exceptions to this principle and may permit that a presentation is not recorded or not published.*

6. Current Publications

6.1. **Springer Contract.** Currently Springer ships 50 or 70 proceedings to each conference. For the new contract, Cachin wonders whether there is still value in receiving proceedings. This year, LaMacchia has already sold 33 proceedings at *Crypto'16*. Pietrzak sold almost all of them for *Eurocrypt'16*. Lai explains (from a Chinese perspective) the benefits of obtaining proceedings at the conference over ordering them online from Springer.

6.2. **Publications administrator.** There is nothing to report.

7. Publications and events

7.1. ***ToSC* status and copyright.** The Board has previously discussed to use a Creative Commons license (CC-BY). Further details will be sent around by email. Cachin prefers to host *ToSC* on an IACR domain (although it will be on a server from RUB).

> Action Point **12: Cachin, Leander, Preneel** *(no time set)*:
> Set the contract for *ToSC* up and ensure the first issue is published.

7.2. **Affiliated events.** Abdalla suggests that affiliated events could draw people to our own conferences. For *Eurocrypt'17* there was a call for affiliated events; it will also be colocated with IEEE's EuroS&P.

Smart suggests that attendees of ICW events should become members. The same suggestion is brought up for sponsored Schools. Another possibility is to give IACR members a discount for these affiliated events.

Rose highlights that the membership dues do not cover any specific costs. He suggests that the fee could be reduced to 0.

LaMacchia points out that we do have fixed costs. Myers adds that video-production etc. costs money as well. Yung posits that there are no other learned societies related to our field with free membership. Orman points out that people need not be a member to be associated with the IACR.

Preneel notices that our stance to make IACR publications freely available has reduced the incentive to remain a member.

7.3. **Registration system support for side-events, workshops etc.** It was discussed that co-locating workshop and related events may should incur some changes to the registration system, as the system may currently only handle registrations for IACR conferences.

8. Conference reports since last BoD Meeting

8.1. ***Eurocrypt'16.*** Pietrzak (GC *Eurocrypt'16*) says that the conference will have made a small loss. He highlights that the professional barista was highly appreciated by attendees.

Cachin thanks Pietrzak for his hard work.

9. Forthcoming Conferences

9.1. ***Asiacrypt'16.*** Lai (obo Hieu) reports that the registration fee is fairly low and that paper acceptances have gone out.

9.2. ***Eurocrypt'17.*** Abdalla (GC *EC'17*) is still working on further sponsors.

9.3. ***Crypto'17.*** Myers (GC *Crypto'17*) remarks that there has been a change of personnel at NSF.

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

10.1. **Asiacrypt Steering Committee.** Lai mentions that there is no further news for *Asiacrypt'17* and *Asiacrypt'18*.

10.2. ***Crypto'18* General Chair appointment.** Several excellent candidates are nominated, and after discussion a candidate is selected.

Decision 6. *Tal Rabin is appointed General Chair for Crypto'18. [Rabin subsequently accepted.]*

10.3. ***CHES* Steering Committee.** Preneel gives an update on the organization of *CHES'16* and explains the details of the *CHES'17* proposal, which is in the repository. He considers the latter a solid proposal.

Decision 7. *The proposal for CHES 2017 in Taipei is approved, with Bo-Yin Yang and Chen-Mou Cheng as General Chairs and Naofumi Homma and Wieland Fischer as Program Co-Chairs.*

10.4. ***FSE* Steering Committee.** Preneel (SC *FSE*) mentions that the *FSE* steering committee is considering a proposal for *FSE'18* and they expect to have a proposal ready well in time.

10.5. ***PKC* Steering Committee.** Pointcheval (SC *PKC*) is still awaiting a proposal for *PKC'18*, but expect one soon.

10.6. ***TCC* Steering Committee.** A proposal for *TCC 2017* in Baltimore (JHU) has been circulated. There are some comments on the venue and budget.

Decision 8. *The proposal for TCC 2017 in Baltimore is approved, with Abhishek Jain as General Chair and Yael Kalai and Leonid Reyzin as Program Co-Chairs.*

Rose inquires after the budget for *TCC16-B*, which takes place soon.

10.7. **Schools Committee (Cryptology Schools).** There are no further things to report; the next submission deadline is August 31, 2016.

11. Closing Matters

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

- By default recordings of presentations.
- The *ToSC* will publish its first issue soon.

11.2. **Review of Action Points.** Skipping the review of action points, Cachin closes the meeting at 17.43.