MINUTES IACR BOARD MEETING *EUROCRYPT'15* (FOR APPROVAL)

SOFIA, BULGARIA, 26 APRIL 2015

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.

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 13 attendees, holding a further 2 proxies, and a number of observers joining for shorter stretches.

Attendees (Elected). Michel Abdalla (Director –2015); Masayuki Abe (Director –2017); Josh Benaloh (Director –2017); Christian Cachin (President –2016) Bart Preneel (Director –2016, *FSE* and acting *CHES* Steering Committees); 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, *TCC* Steering Committee); Brian LaMacchia (GC *Crypto'16*); Svetla Petkova-Nikova (GC *Eurocrypt'15*); Krzysztof Pietrzak (GC *Eurocrypt'16*).

Attendees (Observers). Andrew C. Clark (past president and sage, items 1 and 2.1); SM Yiu (candidate GC *Asiacrypt'17*, item 10.1); Phil Rogaway (chair of Fellows committee, item 3.1).

Absentees (Elected). Tom Berson (Director –2015); Anna Lysyanskaya (Director –2015, proxy Yung); Christof Paar (Director –2016, *CHES* Steering Committee); David Pointcheval (Director –2016, *PKC* Steering Committee, proxy Abdalla).

Absentees (Appointed). Steven Galbraith (GC *Asiacrypt'15*); Phan Duong Hieu (GC *Asiacrypt'16*); Thomas Ristenpart (GC *Crypto'15*). Mike Rosulek (Communications Secretary); abhi shelat (Membership Secretary –2014).

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

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

1.3. **Minutes.** Given the late finalization of the minutes of both the BoD and membership meetings at *Crypto'15*, approval will be postponed to give Board members a chance to read and provide feedback. [The minutes were subsequently approved with some minor changes.]

1.4. **Action Points.** Cachin briefly reviews the status of action items identified from the *Crypto'15* meeting.

(1) The opt-in system for the JoC has not yet been implemented. The action point is retained, with Cachin taking the lead.

> Action Point **1: Cachin** *(no time set)*:
> Implement the JoC opt-in system on the registration and with UCSB/Springer

(2) The *Eurocrypt'16* budget has been approved. Pietrzak (GC *EC'16*) will continue updating the budget and liaise with Rose as the conference comes closer.
(3) The program chair guidelines have been reformulated, see Item 5.3.
(4) Sticky reviews have been incorporated in the proposed new program chair guidelines.
(5) There has been extensive email discussion within the Board, including the program chairs. See Item 5.3 for further discussion.
(6) *Eurocrypt'15* will have mostly parallel sessions. The *Crypto'15* list of accepted papers has not yet been finalized, so the balance plenary versus parallel has yet to be decided.

1.5. ***Eurocrypt'15* Status.**

Petkova-Nikova (GC *EC'15*) mentions that registrations are around 320. There are a fair amount of local attendees and Bulgarian expats returning. There are 15 student speakers with an IACR stipend, two of whom were given a hotel allowance as well. Some further registration waivers were granted to the organization team.

The fee has been lower than originally envisioned as a result of generous sponsorship. No refunds were given after the first of April, although changing the delegate was still allowed. The number of Proceedings provided by Springer is currently higher than the number required.

One comment regarding the registration is that setup is easy, but even small changes need to be dealt with by the Membership Secretary, which is not an optimal workflow. Clark reports he experienced problems with updating his password.

Cachin thanks Petkova-Nikova for her hard work.

2. Officer and Appointee Reports

2.1. **Treasurer's Report.**

Rose has sent out a report, including a breakdown per event, and gives some background information. The IACR is in a good state, though there was a minor operating loss over the combined conferences. He has set up the investment account agreed upon at *Crypto'15*. Clark has been helping with European tax issues and liaising with general chairs.

Rose reports some problems related to tightening of national rules regarding money transfers. His wire transfers to India have been bounced after a month. Clark suggests to register a conference with the appropriate Indian authorities, pointing out that participants should then apply for a conference visa.

Rose continues that *PKC'15* at NIST resulted in certain additional government regulations coming into play, causing complications. From his perspective, these were much worse than anticipated, so he recommends to avoid hosting future events there, if similar regulation would apply.

Cachin thanks Rose for his hard work. The audit committee has not been very active yet; the Board will ask the committee to report at *Crypto'15*.

> Action Point **2: Audit Committee** *(Crypto'15)*:
> Start auditing and provide an interim report

2.2. **JoC Editor in Chief.**

Damgård reports that the JoC has completed its move to a web system for reviewing (and has already resulted in an acceptance!). The supplier is very responsive, with the exception of enabling default `https` access. Franklin will handle all papers that were submitted before the handover. Damgård is waiting for Franklin's view to see if the JoC's publication pipeline is speeding up. About half of the submissions are easy rejects and most solicited conference papers are submitted quite fast. He tries to have physical meetings for editors and will have another one later today.

There is a discussion how to increase the incentive for reviewers to give timely reviews. The best reviewers could be published more prominent, thus increasing their visibility.

> Action Point **3: Damgård, Stam** *(Crypto'15 rump session)*:
> Increase the visibility of good reviewers

Smart mentions that for (e.g. solicited) conference papers, adding a footnote on the first page is not the best place for a reference (as this might hamper ISI indexing). It is suggested to instead incorporate the publication history in the related work section.

According to a report by Garay (PC *Crypto'14*), Algorithmica has invited a number of *Crypto'14* papers to publish in their journal. The Board is of the opinion that ultimately it is up to authors to decide in which journal they wish to publish a full version (if any).

Cachin thanks Damgård for his work.

2.3. **Program chair reports (+Ethics Committee).**

Benaloh says that program chairs are getting better at providing reports. Cachin points out that there is a separate directory on the SVN for these and requests to update there.

> Action Point **4: Benaloh, Cachin** *(1 July 2015)*:
> Migrate relevant PC reports on the SVN

Benaloh mentions that PC chairs are looking more seriously at the potential new PC members list. Stam adds that for workshop chairs, he provides the list and additionally refers to the relevant Steering Committees.

There have been two plagiarism cases on the eprint archive. Both articles have been clearly flagged as such.

Stam inquires what happened with any double submissions flagged up by program chairs. Benaloh will liaise with the program chairs and the relevant authors will be notified accordingly. LaMacchia points out that the PC guidelines could be clarified.

Action Point **5: Cachin, Smart** *(1 July 2015)*:
Clarify the program chair guidelines with regards to the reporting of double submissions.

2.4. **Communications Secretary.** Cachin (obo Rosulek) has posted a report on the SVN and he compliments Rosulek for doing a great job. The Board would need to find a fresh face to maintain the PhD genealogy database.

Action Point **6: Cachin** *(no time set)*:
Find a volunteer to maintain the PhD database

2.5. **Membership Secretary.** Cachin (obo shelat) has no update to give.

3. Internal Committee appointments, reports, and decisions

3.1. **Fellows Committee.** The Fellows for 2015 have been announced earlier in April. All Fellows will receive their plaques at Crypto or Asiacrypt.

Rogaway explains that coming to a consensus is becoming harder with a larger number of candidates entering, ultimately leading to a delay in the announcement of the Fellows. In the presence of many qualified candidates, there was unclarity about the number of Fellows the committee should select.

The Board notices that the long-term target is that about 5% of the membership will be Fellow (currently the number of Fellows is about 3% of the total membership). The Board agrees that if there are many great nominations, the Fellows committee may need to make a selection. However, the "three to five" mentioned on the website is not a hard IACR or Board guideline. As indicated by the historical number of induced nominees, there is no imposed rule on the number of Fellows per year. Rather, the Board leaves the precise numbers of Fellows to be appointed to the Fellows Committee, who may decide on a suitable number from year to year. The Board will ensure consistency between the official guidelines and the website (by changing the website).

Action Point **7: Cachin, Smart** *(1 May 2015)*:
Update the Fellows website to ensure consistency with the official guidelines.

The Board thanks Rogaway and the Fellows committee for their efforts. Gilles Brassard will be chairing the Committee next year.

3.2. **Ethics Committee.** Currently all members of the Ethics committee need to be Board members. There is a discussion on allowing one IACR member on the committee, who may or may not be on the Board. The advantage of this setup is that it increases the pool of candidates to serve.

Decision 1 (unanimous)**.** *The Ethics committee guidelines will be updated to change its constituency to Vice-President, PC liaison officer, and a third person who needs to be a member of the IACR.*

Action Point **8: Cachin, Stam** *(1 July 2015)*:
Update the Ethics Committee guidelines.

Decision 2. *Josh Benaloh (PC liaison), Tom Berson, and Nigel Smart (chair) are appointed to the Ethics Committee for the 2015 calendar year.*

3.3. **Schools Committee.** When funding for Schools was allocated (earlier in April), for one school the decision was referred to the current Board meeting. The pros and cons are discussed, but the Board agrees with the Schools Committee that the proposal is closer to a workshop than a School. Smart mentions that a School should have clearly articulated Intended Learning Outcomes. The Board confirms its decision not to sponsor this School (6 against funding, 6 abstentions). ICW status for this event is left to the President (bearing in mind the following discussion).

There is a discussion regarding discriminatory registration fees. The IACR traditionally supports lower fees for students, members, and in some cases discounts for local participants. The Board considers other forms of discrimination undesirable. In particular, there should not be a distinction between academic and industrial attendees. Discrimination based on the membership of a professional organization can be acceptable. This policy should extend to allowing School funding or ICW status. Preneel mentions that such a policy might be hard to enforce.

Action Point **9: LaMacchia, Stam** *(1 July 2015)*:
Create new phrasing on non-discriminatory fees for the general chair guidelines, which will then be lifted to ICW and Schools.

The Board leaves the initiative for further clarification of the guidelines (for instance the criteria for funding) to the Schools committee. Smart believes the current guidelines are clear enough.

Finally, a new School committee with slightly revised membership is appointed.

Decision 3. *Michel Abdalla (chair), Masayuki Abe, Sasha Boldyreva, Aggelos Kiayias, and Svetla Petkova-Nikova are appointed to the School Committee.*

Cachin recommends Abdalla and the committee for doing a good job.

3.4. **Election Committee.** Cachin notes that the terms for Abdalla, Berson, and Lysyanskaya come to an end this year. The Board unanimously elects an Election Committee as follows.

Decision 4. *Josh Benaloh (chair), David Pointcheval, Bart Preneel (returning officer) are appointed to the Election Committee for the 2015 election.*

4. Program Chair and other appointments

4.1. **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. Preneel suggests to keep people on the list until they have served a number of times, say thrice. Several concrete additions to the lists are made.

4.2. **Crypto'16–'17.** Matt Robshaw has already been appointed as one of the co-chairs for *Crypto'16*. Several excellent candidates are nominated, and after discussion a candidate is selected.

Decision 5. *Jonathan Katz is appointed Program Chair (rolling co-chair) for Crypto'16 and Crypto'17. [Katz subsequently accepted.]*

4.3. **Asiacrypt'16–'17.** Jung Hee Cheon has already been appointed as one of the co-chairs for *Asiacrypt'16*. Several excellent candidates are nominated, and after discussion a candidate is selected.

Decision 6. *Tsuyoshi Takagi is appointed Program Chair (rolling co-chair) for Asiacrypt'16 and Asiacrypt'17. [Takagi subsequently accepted.]*

4.4. **Membership Secretary.** shelat's term officially expired at the end of 2014. Due to his absence, the board defers any decision.

5. Procedures and Guidelines

5.1. **Discussion of needed revisions.** Cachin remarks that there are no revisions beyond those scheduled on the agenda elsewhere or mentioned already.

5.2. **In-cooperation with IACR (ICW).** Cachin has nothing to report, though note the relevant discussion regarding non-discriminatory fees under Item 3.3.

5.3. **Approval of Updated Program Chair Guidelines.** Smart and Cachin have distributed updated program chair guidelines, clarifying the goal of the guidelines and incorporating recent changes. One change is the decision to a unified submission format. There has been no clear feedback from the Steering Committees yet, and the guidelines are amended stating that program chairs of the workshop should contact their respective Steering Committee for any deviations to the submission formatting (in the call for papers).

The Board still needs to come to an agreement on a number of pages. An argument for a longer paper is that it gives authors the opportunity to better express themselves, which makes reading and reviewing easier. An argument in favour of a shorter paper is that the reviewing load will be lighter; longer papers are better submitted to a journal. Eventually, the Board believes 30 pages as page limit is reasonable, while emphasizing that this page limit should not be used as an argument against *shorter* papers.

Decision 7 (2 abstentions, rest in favour)**.** *The updated program guidelines, including the amendments from this meeting, are approved.*

6. Current Publications

6.1. **Publications administrator.** The trial to check uploads of author versions of published papers on eprint is continuing, but Cachin does not know how many uploads have been made on behalf of the authors. Smart observed that for TCC someone centrally (possibly the program co-chairs) must have uploaded papers on behalf of the authors. KU Leuven is using mostly students for the checking, so the costs should not be that high.

Abdalla mentions that extracting good bibliographical data from eprint is difficult to do in an automated manner. Smart reports on some recent software changes to the eprint software by Rosulek that might facilitate Abdalla's job, who is invited to help improve the interface further.

7. Publications and conference strategy

7.1. **Status and plans.** Cachin informs the Board that at *TCC*, Dodis has presented a concrete proposal to change IACR's publication model. It is similar to the Proceedings of the IACR (from the strawman proposal in 2013) but there are some subtle, yet important changes.

The *FSE* steering committee would like to move away from LNCS and adopt the PETS model using a continuous submission model with one annual event. Preneel emphasizes that this entails a proper journal revision model. One argument is that the *FSE* community has a strong European and Asian bias, where journal publications and indexing are considered important.

A potential publisher is DeGruyter (fees are very modest). Dagstuhl is another option, also for archiving. Self publishing is a lot harder. The Steering Committee would hope the Board will facilitate the move, partly by ensuring FSE-style papers will still be welcome at the conferences. The precise link with the other IACR venues and the Journal of Cryptology still has to be fleshed out.

Smart is wondering whether other workshops would be willing to join. The timeline will mean that a firm decision will have to be made this year. The Board is supportive of the ideas and will consult the membership accordingly.

7.2. **Parallel tracks.** There will be parallel sessions for *Eurocrypt'15* and there are approving sounds of the structure chosen by the program chairs. The *Crypto'15* program chairs still appear hesitant, but Cachin is confident that they will be able use parallel sessions to their advantage.

8. Event reports since last BoD Meeting

8.1. ***Crypto'14.*** It happened.

8.2. ***CHES'14.*** Preneel says it was very well organized and resulted in a surplus.

8.3. ***Asiacrypt'14.*** Cachin reports that the conference was a success, Rose reports that the finances have all been done.

8.4. ***FSE'15.*** Preneel believes it went very well. He will ask the organizers to coordinate with IACR's webmasters to reenable the website.

8.5. ***TCC'15.*** Damgård reports it took place and he heard that it went very well. In addition to the already approved *TCC'16* in January in Tel Aviv, the *TCC* Steering Committee is considering a proposal for a second *TCC'16* in November or December. The committee has not yet resolved how to call the likely two *TCC'16* conferences. [Springer later indicated the preferred terminology would be *TCC 2016-A* and *TCC 2016-B*.] The Board authorizes Rose to use merged reporting for the two conferences, if this works out better with the current tools.

8.6. ***PKC'15.*** Yung reports that it went very well. Rose notices that due to the location (NIST), participants had experienced some additionally administrative overhead. LaMacchia points out that for US citizens there were some ID compliance issues (requiring passports instead of driver licenses).

9. Forthcoming Conferences

9.1. ***Crypto'15.*** Cachin (obo Ristenpart (GC *C'15*) reports everything is fine.

9.2. ***Asiacrypt'15.*** Cachin (obo Galbraith GC *AC'15*) reports the budget has been revised and everything is under control.

9.3. ***Eurocrypt'16.*** Pietrzak (GC *EC'16*) reports everything is on track. There will not be a general co-chair. He has applied for some assistance from IST for administrative support and he will enlist his group for operational support during the conference.

Parallel tracks will be supported. A setup for synchronized audio plus powerpoint recording can be provided for 900€ per room, but this excludes operating and editing.

9.4. ***Crypto'16.*** LaMacchia has some ideas for special touches. It will be at UCSB.

9.5. ***Eurocrypt'17.*** There is no proposal yet. Various past potential candidates have ruled themselves out for 2017. Abdalla mentions the possibility to host in Paris, France. Cachin encourages a full proposal, at the latest by *Crypto'15*.

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

10.1. **Asiacrypt Steering Committee.** SM Yiu gives a clear presentation for a proposal to host *Asiacrypt'17* in Hong Kong. Yiu explains the budged in some more detail. He confirms that the University will be able to host parallel sessions and has the technical facilities to record (and edit) technical presentations.

Cachin thanks Yiu for the work that went into the preparation of this proposal.

The Board unanimously accepts the proposal.

Decision 8. *Asiacrypt 2017 will be held in Hong Kong (Hong Kong) and Duncan Wong and SM Yiu are appointed General co-Chair.*

Yiu will take the place on the Board.

10.2. ***CHES* Steering Committee.** Preneel (SC *CHES*) mentions that according to the three year cycle, the plan is to have *CHES 2016* co-located with *Crypto'16* at UCSB. The CHES Steering Committee has decided on general and program co-chairs, however there is no budget yet. As a result, the following decision is conditional on receiving a budget.

Decision 9. *The Board approves the CHES 2016 proposal, meaning that CHES 2016 will be held at UCSB (USA) with Çetin Kaya Koç and Erkay Savaş as General co-Chairs and Benedikt Gierlichs and Axel Poschmann as Program co-Chairs.*

Action Point **10: Preneel, Paar** *(Crypto'15)*:
Present an updated budget for *CHES 2016*.

LaMacchia (GC *Crypto'16*) asks about the arrangements of past co-located events.

10.3. ***FSE* Steering Committee.** Preneel (SC *FSE*) has nothing further to report.

10.4. ***PKC* Steering Committee.** Pointcheval (SC *PKC*) mentions that everything is on track. There is a solid proposal for *PKC 2017* to be hosted in Amsterdam.

Decision 10 (Unanimous)**.** *The Board approves the PKC 2017 proposal, meaning that PKC 2017 will be held in Amsterdam (the Netherlands) with and Marc Stevens as General Chair and Serge Fehr as Program Chair.*

10.5. ***TCC* Steering Committee.** Yung (SC *TCC*) has nothing further to say.

11. Closing Matters

11.1. **Draft Agenda for Membership Meeting.** Cachin quickly recapitulates the main issues to discuss at the membership meeting, namely parallel sessions and the FSE publication model (bearing in mind that at the end of the year we need to renegotiate our publishing contract).

11.2. **Review of Action Points.** After a review of action points, Cachin closes the meeting at 17:46.