MINUTES IACR BOARD MEETING *CRYPTO'14*

SANTA BARBARA, 17 AUGUST 2014

1. Opening Matters

At 9.10 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. **Roll of Attendees.** There are 16 attendees, holding a further 5 proxies.

Attendees (Elected). Michel Abdalla (Director –2015); Josh Benaloh (Director –2014); Tom Berson (Director –2015); Christian Cachin (President –2016) Shai Halevi (Director –2014, TCC Steering Committee); Anna Lysyanskaya (Director –2015); Christof Paar (Director –2016); David Pointcheval (Director –2016, PKC Steering Committee). Bart Preneel (Director –2016, FSE Steering Committee); Greg Rose (Treasurer –2016); Nigel Smart (Vice-President –2016); Martijn Stam (Secretary –2016); Moti Yung (Director –2014).

Attendees (Appointed). Alexandra Boldyreva (GC *Crypto'14*); Thomas Ristenpart (GC *Crypto'15*).

Attendees (Representatives and Others). Mike Rosulek (Observer; from 15.00); Krzysztof Pietrzak (Observer; prospective EC'16 general chair); Hilarie Orman (Archivist); Philip Rogaway (Observer; from 15.30). Kenny Paterson (Observer; proxy for Galbraith);

Absentees (Appointed). Ivan Damgård (Journal Editor-in-Chief –2016, proxy Smart); Steven Galbraith (GC *Asiacrypt'15*, proxy Paterson); Matt Franklin (Journal Editor-in-Chief –2014, no proxy); D.J. Guan (GC *Asiacrypt'14*); Gregor Leander (GC *Eurocrypt'14*); Svetla Petkova-Nikova (GC *Eurocrypt'15*, proxy Preneel); abhi shelat (Membership Secretary –2014, proxy Halevi).

Absentees (Representatives and Others). San Ling (Asiacrypt Steering Committee, proxy Cachin); Jean-Jacques Quisquater (CHES Steering Committee, proxy Paar).

1.2. **Minutes.** The minutes of both the BoD and membership meetings at *Eurocrypt'14* are approved with some minor changes.

1.3. **Action Points.** Cachin briefly reviews the status of action items identified from the *Eurocrypt'14* meeting. The majority of action points are either completed or still pending with little progress to report. However, for a few additional information is available.

Regarding program chairs, Cachin remarks that he has included Benaloh to the communications with prospective program chairs and helped him with the chasing of past chairs for reports. Program chair guidelines have been updated, but still need formal approval by the Board, which is granted.

Decision 1. *The new program chair guidelines are unanimously approved.*

Orman mentions that the archiving guidelines in there still need updating. Benaloh reckons after today's meeting further changes might be needed.

Regarding publications, a system to move to JoC opt-in is not yet in place.

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

Smart has been hoping to open up the eprint archive to author versions of papers where IACR does not hold the copyright. However, his attempts to contact IEEE have been fruitless so far.

1.4. ***Crypto'14* Status.** Boldyreva (GC *C'14*) hopes everything will go smoothly. The number of registrations is expected to be close to 400. The rump session room will be used for the first two days. There was no reason from an organization perspective to have parallel sessions. She only established the registration fee after the program chairs clarified the program needs.

Cachin thanks Boldyreva for her hard work.

2. Officer and Appointee Reports

2.1. **Treasurer's Report.** Rose has sent out a report and gives some background information. The IACR is in a good state. Cachin thanks Rose for his hard work.

Cryptography Research Inc. has donated a large sum to the IACR for the Cryptography Research Fund for Students; this was negotiated by Paul Kocher. It is unclear whether the fund can be used in perpetuity or needs to be spent within a set timeframe. There is a discussion within the Board what would be preferred. The suggestion is to have a subcommittee of the Board to establish a more explicit policy to ensure the fund is used to good effect.

Rose has talked to WFA about an investment fund for part of the reserve. It is an extremely conservative portfolio with significant control on the mix by the IACR. Paar points out that there is still a risk involved and Rose asks the Board for guidance on the level of risk desired and acceptable. The Board is in favour of the mix that involves a small percentage of stocks (proposal 3).

In order to progress with the WFA investment account, a Board resolution is required. A formal phrasing of the required resolution has been circulated beforehand. Rose points out that the Authorized Individuals need to be IACR Directors with US Green Card or Passport.

Decision 2 (17 in favour, 1 abstention)**.** *The resolution as circulated beforehand is approved, the Authorized Individuals will be Greg Rose in first instance, with Tom Berson as a back up.*

Decision 3 (Unanimous)**.** *The Board appoints Michel Abdalla, Josh Benaloh, Tom Berson, Christian Cachin, Helena Handschuh, and Greg Rose to the Endowment Committee*

2.2. **JoC Editor in Chief.** Cachin (obo Franklin and Damgård) reports that the new website has launched, which has triggered the handover between Franklin and Damgård.

2.3. **Program chair reports (+Ethics Committee).** Smart mentions that the PC Liaison officer is part of the Ethics committee. Otherwise there is nothing to report.

2.4. **Membership Secretary.** Cachin (obo shelat) gives an update on membership figures. The IACR currently has 1437 members.

2.5. **Archivist.** Orman explains the process, which is now very simple. Nonetheless, most of her time is spent chasing program chairs. IEEE has a new system to find plagiarism and similarities. They check both whether papers are based on other works, but also whether other works plagiarized their papers. The question is whether IACR should contact IEEE for collaboration. The Board suggests she does.

Cachin thanks Orman for her work and reports.

3. Internal Committee appointments, reports, and decisions

3.1. **Ethics Committee.** Discussed already.

3.2. **Schools Committee.** Cachin reports that the Schools Committee has received proposals and has a suggestion to the Board regarding the funding. Abdalla clarifies that two schools that were held this July did apply, but our timeline did not allow funding. Of the three suggested schools, one is a new school, two others are already established.

Decision 4 (12 in favour, 5 abstentions)**.** *The Board adopts the proposal by the Schools Committee, meaning that three schools will be supported with 5k$ each.*

Lysyanskaya asks Abdalla about the process by which the Schools Committee came to its recommendation and whether the guidelines can be clarified to reduce the potential for politics playing a factor in allocating funding.

Cachin thanks the committee for its efforts.

3.3. **Election Committee.** Preneel has finalized and made available a nomination form. The election committee is talking to potential candidates to serve on the IACR Board of Directors.

4. *Eurocrypt 2016* proposal

Pietrzak gives a clear presentation where he clarifies that there will likely be a co-chair, but it is not yet clear who. Yung points out that CCS 2016 will be in Vienna (in September). The Board provides some general feedback and unanimously accepts the proposal conditionally, noting that the budget is still missing.

Decision 5. *Eurocrypt 2016 will be held in Vienna (Austria) and Krzysztof Pietrzak is appointed General Chair.*

Action Point **2: Pietrzak** *(End of September 2014)*: Present an updated budget for Eurocrypt 2016.

5. Program Chair and other appointments

5.1. **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. Several suggestions are made and the lists will be updated accordingly.

5.2. **Eurocrypt'16–'17.** Marc Fischlin has already been appointed as one of the co-chairs for *Eurocrypt'16*. Several excellent candidates are nominated, and after discussion a candidate is selected.

Decision 6. *Jean-Sébastien Coron is appointed Program Chair (rolling co-chair) for Eurocrypt'16 and Eurocrypt'17. [Coron subsequently accepted.]*

5.3. **Eurocrypt 2016 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 7. *Bart Preneel is invited to deliver the Distinguished Lecture at Eurocrypt'16. [Preneel subsequently accepted.]*

6. Guidelines

6.1. **Discussion of other needed revisions.** Cachin remarks there are no further revisions needed.

7. Experience with the Program Co-Chair model

Cachin gives a small summary of the comments received from past program co-chairs. The general feedback is overall positive: it leads to balance and continuity. He does have the impression that mostly chairs of *Crypto* seem to have issues with the model. The negative aspects relate to a longer time commitment stretched over two years and to a lack of clear decision power. Smart mentions that the system was only truly in place from 2012 onwards. Abdalla would like to have feedback from PC members as well.

One concern is the load for two consecutive years. Paar explains that for *CHES* the co-chair model is different (not-rolling), but it works well. He would prefer to move to a *CHES*-like model. Yung adds his experience from having served as CCS program co-chair. There is a belief that chairing a flagship conference does not necessarily compare to chairing a workshop. One potential advantage of rolling co-chairs is the learning experience, which might explain part of the added benefit.

Halevi recalls that he was overwhelmed at the time he was program chair, he believes there should be a junior/senior model. Lysyanskaya wonders whether a weaker model is possible by making the chair designate an omnipresent PC member. Benaloh and Preneel remark that this was tried in the past but led to marginalization of the chair designate.

Smart believes the current model works very well for *Eurocrypt* with complementary expertise. Yung remarks that with the rolling co-chair model we might relax the informal rule regarding matching chairs to continents. This would allow a better matching in area, given that not all regions are equally represented in all domains.

> Action Point **3: Smart and Cachin** *(no time set)*:
> Revise the formulation of the co-chair paragraph in the program chair guidelines.

8. Current Publications

8.1. **Publications administrator.** With the help of an administrative staff member at KU Leuven, Cachin and Preneel have started to track which conference papers already have been uploaded as author version on the eprint. The current (free) trial only started recently, so it is not yet clear how much time all the checking and chasing will take, nor what the eventual costs will be.

Orman points out that some of this work can be automated. Cachin responds that this would require updating the eprint software. There is an ensuing discussion about metadata and the consistency of data in IACR's systems (and beyond).

9. Publications and conference strategy

9.1. **Publications format.** Smart has discussed the publication process with various active members. There seems to be agreement on sticky reviews as part of supplementary material to papers (as an option for the author). Halevi remarks that he allowed these when he ran *Crypto*, yet noone used the opportunity.

Decision 8. *Sticky revisions are encouraged.*

> Action Point **4: Smart and Cachin** *(no time set)*:
> Make a clear policy regarding sticky reviews and communicate with the program chairs.

Smart continues that the issue of multiple formats was more contentions. What is being submitted, what is being reviewed, and what is being published currently differ. In an attempt at unification, the *Eurocrypt'15* program chairs experimented in their call for paper, with some critical comments from the program committee.

Halevi argues that, even without a page limitation, he would format a submission differently as an eprint. Yung believes a submission should be in the best format for the reviewers to review. Committees are time constrained and he would format differently for time-constrained readers than for readers with time.

Preneel does not believe it benefits the community. He favours to publish what is reviewed, and review what is submitted. Cachin considers harmonization between submissions and publications as more honest to the community as the extra work currently put in by authors might prove a waste. Moreover, he believes that an unlimited page limit will harm the field as we can no longer review the full submissions and this lack of full reviews will show.

Smart points out that the formally published version is the one that matters for funding agencies etc. He notices that depending on the type of paper you are writing (influencing the balance between text, pictures, formulae, etc.), the difference between LNCS style and other styles can be more or less pronounced. He advocates that submissions are already in LNCS format and supplementary material appears as an additional file or after a page limit.

All considering, the Board would like to move to a situation where the submission format is similar to published version (same style file etc.) The suggestion is to discuss this proposal at the membership meeting and call for a straw poll from the membership.

> Action Point **5: Smart and Cachin** *(no time set)*:
> Work with program chairs to move towards harmonizing submission and publication format.

For information, Springer has given an updated quote for Gold Open Access which is based on the number of pages. There is a discussion whether we should open negotiation with other publishers.

The indexing of the Journal of Cryptology has gone down drastically and a discussion ensues without clear resolution.

9.2. **Parallel tracks.** With the increased number of papers, the Board has been actively seeking guarantees from general chairs for the option of parallel sessions. However, so far program chairs have preferred shorter talks and denser programs. Taking up Cachin's proposal to move to parallel tracks, which was circulated before the meeting, Smart suggests a one-year experiment with parallel tracks at the three conferences. It is feasible for the 2015 conferences. After that there will be a vote by the membership.

Benaloh suggests mandating parallel sessions whenever the number of papers exceeds a certain threshold (say 40). Boldyreva wonders the extent of parallellism that will be involved. There is a discussion about inequality if part of the program is plenary, and part parallel.

Orman believes parallel sessions will be chaotic to implement and sorting out how to do it well will take more than one year. She does not believe there is sufficient support for such an experiment.

Halevi would like to phrase the 'parallellism' requirement in a way that is minimally evasive to the program co-chairs. He suggest to say explicit what not to have.

Cachin mentions restricting the duration of the conference. He thinks that a less dense program would allow for more interaction among attendees and create room for alternatives within the program (e.g., workshops or tutorials).

Decision 9 (14 in favour, 1 against)**.** *The three flagship conferences in 2015 shall have a significant portion of parallel sessions.*

> Action Point **6: Cachin** *(no time set)*:
> Talk to Program and General Chairs of 2015 about implementing parallel sessions.

10. Fellows Committee

In 2014 there was an ambiguity in the wording of the rules of the Fellow guidelines (regarding who needs to be an IACR member and in which year). Rogaway clarifies that the Fellows Committee requests a relaxation of the membership requirement for nominees, nominators, and endorsers.

There is a discussion of the pros and cons of these restrictions. Preneel believes the nominator should be a member, as well as at least one endorser. He expresses his concern that some Fellows do not engage with the community. Berson asks what the role of a Fellow is: is it primarily a recognition of past achievement, or do Fellows also have an ambassadorial role for the society. Yung remarks that some Fellowships have been awarded based on past performance, not on current engagement. Orman wonders whether the Fellows Committee feels it is part of the IACR.

Decision 10 (17 in favour, 1 abstention)**.** *The Fellowship guidelines will be updated as follows: a nominee must be a member, a nominator must be a member or Fellow, and at least one of the endorsers should be a member. In this context member means in the current or the previous year.*

Decision 11 (15 in favour, 2 abstentions)**.** *At the discretion of the Fellows Committee, a candidate nominated in a given year may be reconsidered as if freshly nominated for a Fellowship for either of the following two years without any need for resubmission, provided that all other conditions are satisfied at the time of reconsideration.*

11. Communications Secretary Position

After six years of Newsletter Editor, Wolf has stepped down. Mike Rosulek and Yu Yu are currently already serving as IACR webmaster (together with McCurley and Cachin). Rosulek would like to serve on the Board as Communications Secretary. He discusses the challenges he sees in this role, leading to a more general discussion about the generation of content and the extent to which content is being read.

Decision 12 (18 in favour)**.** *Mike Rosulek is appointed Communications Secretary from August 2014 to (and including) December 2016.*

12. Event reports since last BoD Meeting

12.1. ***Eurocrypt'14*.** Leander is absent, the conference was a success.

13. Forthcoming Conferences

13.1. ***Asiacrypt'14*.** Cachin (obo Guan, GC *AC'14*) confirms it will happen in Taiwan. There are no updates.

13.2. ***Eurocrypt'15*.** Preneel (obo Petkova-Nikova, GC *EC'15*) confirms it will take place as planned. There are no updates.

13.3. ***Crypto'15*.** Ristenpart (GC *C'15*) promises to try to make things happen.

13.4. ***Asiacrypt'15*.** Paterson (obo Galbraith GC *AC'15*) reports that there is nothing to report.

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

14.1. **Asiacrypt Steering Committee.** Nothing to report.

14.2. ***Crypto'16* General Chair appointment.** Several excellent candidates are nominated, and after discussion a candidate is selected.

Decision 13. *Brian LaMacchia is appointed General Chair for Crypto'16. [LaMacchia subsequently accepted.]*

14.3. ***CHES* Steering Committee.** Quisquater (SC *CHES*) has sent a report to the svn. Quisquater steps down from his position after this meeting and had initially planned to attend. Cachin thanks him (in absence) for his dedication to the IACR and his efforts.

14.4. ***FSE* Steering Committee.** Preneel (SC *FSE*) presents a proposal to hold FSE in Germany in 2016. The steering committee has not yet decided on a recommended program chair. Preneel believes it to be a good and financially solid proposal.

The Board unanimously accepts the proposal.

Decision 14. *The Board approves the FSE 2016 proposal, meaning that FSE 2016 will be held in Bochum (Germany) with Gregor Leander as General Chair.*

14.5. ***PKC* Steering Committee.** Pointcheval (SC *PKC*) has nothing new to report.

14.6. ***TCC* Steering Committee.** Halevi has nothing to report.

15. Closing Matters

15.1. **Draft Agenda for Membership Meeting.** Cachin quickly recapitulates the main issues to discuss at the membership meeting: (1) Publications; (2) Conferences; (3) Services; (4) Communications Secretary; (5) Cryptology Schools; (6) Publications and conferences; (7) Membership report; (8) Financial report; (9) Future events.

15.2. **Review of Action Points.** After skipping a review of action points, Cachin closes the meeting at 18.08.

16. Intermediate Board Decisions

Decision 15 (30 October 2014)**.** *The Board approves the FSE Steering Committee's recommendation of Thomas Peyrin as Program Chair for FSE 2016.*

Decision 16 (9 March 2015)**.** *The Board adopts the proposal by the Schools Committee, meaning that two schools (the SAC Summer School in Sackville, Canada, and the School on Computer-Aided Cryptography in Maryland, USA) will be supported with 5k$ each.*

Two further schools are granted "In Cooperation with IACR" status.

Decision 17 (23 March 2015)**.** *The Board approves the TCC 2016 proposal, meaning that TCC 2016 will be held in Tel Aviv (Israel) with Ran Canetti and Iftach Haitner as General co-Chairs and Eyal Kushilevitz and Tal Malkin as Program co-Chairs.*

It was noted that the TCC steering committee plans to move its dates from its current timeframe of Feb-March to a Nov-Dec slot in the long run. The approved proposal will be for TCC in January, moving half-way. As part of the migration, there might be a second TCC towards the end of 2016.