MINUTES IACR BOARD MEETING *EUROCRYPT'13*

ATHENS, 26 MAY 2013

1. OPENING MATTERS

At 10.08 Preneel opens the meeting and he briefly goes around to confirm attendees and establish 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 11 attendees, holding a further 12 proxies.

Attendees (Elected). Michel Abdalla (Director –2015); Josh Benaloh (Director –2014); Christian Cachin (Vice-President –2013) Mitsuru Matsui (Director –2013); Bart Preneel (President –2013, FSE Steering Committee); Greg Rose (Treasurer –2013); Nigel Smart (Director –2014); Martijn Stam (Secretary –2013).

Attendees (Appointed). Aggelos Kiayias (GC *Eurocrypt'13*, for Agenda Item 1 only, proxy Cachin for the remainder); Gregor Leander (GC *Eurocrypt'14*); abhi shelat (Membership Secretary –2014);

Attendees (Representatives and Others). San Ling (Asiacrypt Steering Committee);

Absentees (Elected). Tom Berson (Director –2015, proxy Smart); Shai Halevi (Director –2014, TCC Steering Committee, proxy Smart); Anna Lysyanskaya (Director –2015, proxy shelat); Christof Paar (Director –2013, proxy Leander); David Pointcheval (Director –2013, PKC Steering Committee, proxy Abdalla);

Absentees (Appointed). Alexandra Boldyreva (GC *Crypto'14*, proxy Kiayias); Matt Franklin (Journal Editor-in-Chief –2014, proxy Smart); D.J. Guan (GC *Asiacrypt'14*, proxy Lin); Helena Handschuh (GC *Crypto'13*, proxy Preneel); Satyanarayna Lokam (GC *Asiacrypt'13*); Christopher Wolf (Newsletter Editor –2014, proxy Leander).

Absentees (Representatives and Others). Kevin McCurley (Database Administrator); Hilarie Orman (Archivist). Jean-Jacques Quisquater (CHES Steering Committee, proxy Rose).

1.2. **Minutes.** The minutes of both the BoD and membership meetings at *Crypto'12* are approved with some minor changes. There is a call to get the minutes out earlier, with an announcement by email.

1.3. **Action Points.** Preneel briefly reviews the status of action items identified from the *Crypto'12* meeting. Many items were not addressed and will be retained (in somewhat slightly different formulations) and with updated due dates.

(1) (Web-interface for the JoC reviewing process.) A proposal will be discussed at Agenda Item 5.5.
(2) (Springer contact.) There has been a lot of progress on the new contract, but there are still a few details to be worked out.

> Action Point **1: Publication Committee** *(1 July 2013)*:
> Finalize the implementation of the new contract.

(3) (Membership discussion forum.) Originally the task (to find a forum moderator) was assigned to McCurley, but new insights indicate there is a more substantial IT problem, which needs resolving first.

> Action Point **2: IT Committee** *(1 August 2013)*:
> Suggest a solution for a membership discussion forum.

(4) (Committee membership.) Stam reports no progress.

> Action Point **3: Stam** *(1 August 2013)*:
> Keep better track of all the various committees.

(5) (Update the conference budget template). Rose reports no progress.

> Action Point **4: Rose** *(1 August 2013)*:
> Update the conference budget template to deal better with student stipends and free attendees.

(6) (Update PC guidelines). Stam reports no progress.

> Action Point **5: Stam** *(1 July 2013)*:
> Add the bandwidth and balance expectations to the PC guidelines.

(7) (Create a PC leaflet). Benaloh reports no progress.

> Action Point **6: Benaloh** *(1 July 2013)*:
> Make a 1 page update on recent IACR policy changes for program chairs.

(8) (Collate task lists) Preneel reports no progress.

> Action Point **7: Preneel** *(1 August 2013)*:
> Think about the tasks that the officers and appointed directors have to perform.

(9) (Conference videoing) No concrete progress has been made.

> Action Point **8: McCurley and Cachin** *(1 August 2013)*:
> Find somebody responsible for overseeing consistency of the recording and archiving of videos of presentations at IACR events.

(10) (Archiving of documents) No progress is reported.

> Action Point **9: Cachin and Stam** *(1 July 2013)*:
> Archive the audit committee document and the board voting guidelines.

(11) (Archiving of documents) No progress is reported.

> Action Point **10: Benaloh** *(1 June 2013)*:
> Update the evoting guidelines by uploading to svn.

(12) (Ethics awareness) The campaign is ongoing.

> Action Point **11: Ethics Committee** *(1 June 2013)*:
> Increase awareness of ethics by writing a news item on the official announcement channel.

(13) (*CHES'13* budget) This has been completed.
(14) (Policy on Archiving) No progress is reported.

> Action Point **12: Orman and Stam** *(1 September 2013)*:
> Make a policy on what (photos etc.) the IACR should archive and how, including dealing with permissions.

(15) (Plagiarism detection) No progress is reported.

> Action Point **13: Orman** *(1 August 2013)*:
> Investigate and/or create a tool to detect plagiarism of IACR copyrighted material.

1.4. ***Eurocrypt'13* Status.** Kiayias (GC *EC'13*) reports that there are a good number of students who got their registrations waived, many of whom will be helping out the organization. These waivers were mainly enabled by our generous sponsors. Current registration numbers (just over 300) indicate the financial situation is under control. Kiayias also unveiled the conference gift, including a short tutorial. The contact with the program co-chairs was very smooth.

2. Officer's Report for Approval

2.1. **Treasurer's Report.** Rose has sent out a report and gives some background information. A couple of conferences from last year have not yet finalized. Rose initiates a discussion on the membership fee. He brings forward to possible reasons for change. Firstly, when the Journal of Cryptology becomes opt-in, how should this be reflected in the membership fee: should it be lowered accordingly, should there be differentiation based on receiving the Journal or not. He will table a number of proposals and ask the membership for an opinion.

Secondly, there was a suggestion from Diffie to give retired members a membership for life (rather than expecting them to renew a personal membership every year). Rose recalls the situation by fellow organisation ACM, which has a rule that 55 year old members can pay for 10 years to become a member for life (for members 65 year old, paying for an additional 5 year suffices). The Board feels favourably towards a life membership and has a discussion regarding the way to implement it.

Decision 1. *The Board will initiate a Bylaws change to make life membership possible under the conditions that a member*

- *is 65 year old (or over);*
- *has accrued 20 years of membership (membership years need not be consecutive and both student and full membership count); and*
- *personally requests a membership for life.*

The membership of life itself will be free of charge, but for certain optional services (such as receiving a printed copy of the journal) the costs can still be charged.

> Action Point **14: Preneel** *(no time set)*:
> Prepare a change to the Bylaws to incorporate life membership.

Rose mentions he is currently concentrating on the basic treasury jobs with limited attention for strategic renewal. Preneels recognizes a treasure's job is a busy one and assures Rose that he is doing an excellent job.

3. Guidelines for Approval

3.1. **General chair guidelines.** Rose remarks that no updates have been made.

3.2. **Program chair guidelines.** The new publishing workflow has not been incorporated yet, as it is not quite finalized yet. Once it is completely sorted out, the new workflow needs to be incorporated.

> Action Point **15: Benaloh** *(no time set)*:
> Ensure program chairs are aware of the new publication pipeline, including the requirement to use IACR's submission system.

3.3. **Discussion of other revisions needed.** Cachin is not aware of a further need for changes.

4. Appointees Reports for Information

4.1. **Newsletter.** Preneel (obo Wolf) reports that the Newsletter frequency has gone down, but there is plenty of news on the channel (displayed on the IACR homepage). It is noted that the Newsletter takes a reasonably prominent place in the Bylaws as an obligatory means for the Board to keep the membership informed of important decisions etc. Perhaps this is no longer as relevant as it once was. In general there should be a corner on the website where the Board's policy decisions can easily be seen.

4.2. **JoC Editor in Chief.** Preneel (obo Franklin) reports that the number of papers being submitted to the Journal of Cryptology is still quite low.

shelat (obo Lysyanskaya) champions that the JoC will have special issues for full versions attached to conferences. So far special issues have been more topic based, rather than event based. There is some disagreement, as having event-based issues might have a negative effect on the JoC's ISI status.

4.3. **Membership Secretary.** shelat is working on the conference system to make it easier to set up new conferences. He would like to enable GCs to do more by themselves (without Board intervention). shelat mentions he would like to modernize some of the back-end as well.

> Action Point **16: Cachin and shelat** *(no time set)*:
> Look at the authentication system used for conference registration etc.

4.4. **Archivist.** Preneel (obo Orman) does not believe there is anything to report. shelat is interested in investigating the use of latex of past proceedings to try to create a PDF that works on kindle.

4.5. **Database and Website.** Preneel (obo McCurley) refers to Agenda Item 5.2.

5. Internal Committee Reports for Information

5.1. **Fellows Committee.** There are several new Fellows, who all have elected to receive their plaque at *Crypto'13*. [Lars Knudsen later changed his preference to *Asiacrypt'13*.]

5.2. **Publication and Web Infrastructure.** There have been various calls to discuss publication and web infrastructure. Preneel reports that Springer no longer updates the reading room, but it has freely made available a large number of past proceedings. For the more recent, missing proceedings, a system with access tokens will be used. Halevi has received access tokens from Springer. The new situation should be announced at the upcoming membership meeting.

There is a discussion on the overall state of the current IT system. Up to now, development and maintenance relied on volunteer efforts and IACR's current IT landscape consists of many systems that are somewhat disjointed and many of which show their age and need updating. There seems consensus that creating one big system as a replacement is not desired, but rather increase the interoperability between the various subsystems. How to do the latter is still topic of debate. Several issues and questions are raised, also related to to what extent outsourcing is an option. When parts of the system are outsourced separately, should certain interface and authentication formats be defined (and imposed) to increase interoperability? The fundamental question when outsourcing is who is in control. The IACR's reliance on third parties (e.g. for maintenance) should be reduced as much as possible (so that a switch to another third party is not problematic) and the IACR should maintain ownership of all the metadata involved.

See also Agenda Item 12.1 for further strategic discussion on the future of publications.

5.3. **Ethics Committee.** Cachin has nothing to report.

5.4. **Election Committee.** Benaloh has nothing to add to the report submitted to the Board.

5.5. **JoC web system evaluation.** A small committee has investigated several options; a summary was presented by email. The suggested option is to pay the company that is also responsible for Springer's webreview system. It is noted that as part of the negotiations, the company needs to be made aware of intended changes to the IACR back end. The Board supports this proposal and makes available financial means accordingly.

Decision 2. *The IACR's Journal of Cryptology will move to a web-based submission and review system. The IACR makes available 5k per year.*

Action Point **17: Franklin** *(no time set)*: Start with the adaptation of a web-based system.

Action Point **18: Preneel** *(no time set)*: Speak to Springer to adapt the Journal contract will support our intended infrastructure.

6. APPOINTMENTS

6.1. **Election Committee.** Preneel notes that this year will be a large election, as in addition to 3 Directors there are also 4 Officials that need to be elected. The Board elects an Election Committee as follows.

Decision 3. *Michel Abdalla, Josh Benaloh, and Tom Berson are appointed to the Election Committee for the 2013 election.*

6.2. **Journal of Cryptology Editor-in-Chief.** While Franklin's second term will run out at the end of next year. To promote a smooth transition, the search for a successor should commence. To this end, the following committee is appointed, tasked with recommending a new Editor-in-Chief to the Board.

Decision 4. *Shai Halevi, Nigel Smart, and Bart Preneel are appointed to the JoC-EiC search committee.*

7. CONFERENCES SINCE LAST BOD MEETING

7.1. ***Crypto'12.*** Rose (obo Yin, GC *C'12*) mentions that *Crypto'12*'s finances have all been closed.

7.2. ***Asiacrypt'12.*** Lin (obo Lai, GC *AC'12*) mentions that there are still some outstanding issues, to be discussed at *Crypto'13*.

8. FORTHCOMING CONFERENCES FOR INFORMATION

8.1. ***Crypto'13.*** Preneel (obo Handschuh, GC *C'13*) reports that the colocation with CHES is a lot harder to coordinate than the previous colocation (in 2010). There will be a discount for those who attend both events. CHES is organizing tutorials.

8.2. ***Asiacrypt'13.*** Lin (obo Lokam, GC *AC'13*) mentions that everything seems to be on track. Preneel reminds the Board of the longstanding tradition to promote local participation using IACR funded stipends in countries where the full registration fee would otherwise cause an undue barrier to attendance. The general chair has 5000 USD available for this purpose and is requested to incorporate this funding in the conference budget. Whether the program chairs have considered parallel sessions is unclear at this point.

8.3. ***Eurocrypt'14.*** Leander (co-GC *EC'14*) says his team have updated the website and they are starting to receive sponsoring.

8.4. ***Crypto'14.*** Preneel (obo Boldyreva, GC *C'14*) conveys Boldyreva's apologies; she might not be able to make the board meeting at *Crypto'13* either.

8.5. ***Asiacrypt'14.*** Lin (obo Guan, GC *AC'14*) says the venue has been confirmed. Parallel sessions are possible, but would be some 18 floors apart. The general chair seems to be very responsible and responsive.

9. STEERING COMMITTEE REPORTS AND WORKSHOP PROPOSALS

There is a general concern that the workshops' steering committees are not as well represented at the Board meetings as they could be.

9.1. **Asiacrypt Steering Committee.** Lin mentions that proposals for *Asiacrypt'16* will be discussed at *Asiacrypt'13*.

9.2. ***TCC'13* Report.** Preneel (obo Halevi) has little to add to the detailed report by Goldreich that was distributed prior to the Board meeting.

9.3. ***FSE'13* Report.** Preneel (SC *FSE*) notices that *FSE'13* in Singapore went smoothly. There is an advanced proposal to hold *FSE'14* in London. A ballot (by email) confirming the proposal by the Board is to be expected soon.

9.4. ***PKC'13* Report.** Abdalla (obo Pointcheval, SC *PKC*) reports that *PKC'13* went well. The proposal for *PKC'14* (Buenos Aires, Argentina) has already been approved. The steering committee has tentatively scheduled *PKC'15* to be held at NIST (in Washington D.C., USA) with potential chairs Jon Katz and Rene Peralta. For *PKC'16* the plan is to head back to Asia.

9.5. ***CHES'12* report and *CHES'14* proposal.** Preneel (obo Quisquater, SC *CHES*) mentions that Stefan Mangaard chairs the CHES steering committee very well. The proposal for *CHES'14* is solid and has been thoroughly checked.

Decision 5. *The Board approves the CHES'14 proposal, meaning that CHES 2014 will be held in Korea with Kwangjo Kim as General Chair and Lejla Batina and Matt Robshaw as Program co-Chairs.*

10. CONFERENCE PROPOSALS FOR DISCUSSION/SELECTION

10.1. ***Asiacrypt'15.*** Steven Galbraith (joining the meeting via Skype) gives a very clear presentation for a proposal to hold *Asiacrypt 2015* in Auckland, New Zealand. He confirms that there is a good opportunity to accommodate a larger number of talks using parallel sessions. Lin (SC *AC*) reports that the Asiacrypt steering committee received the proposal positively.

The Board unanimously accepts the proposal.

Decision 6. *Asiacrypt 2015 will be held in Auckland (New Zealand) and Steven Galbraith is appointed General Chair.*

Following the decision, Preneel notices that it would be good to have demographic information (and attendee numbers) available online. After some quick thought showering, interesting data could include (but need not be limited to) total membership, student membership, statistics by continent, the number of countries represented, the top ten countries by membership, the number of papers published, the relevant impact factors, and acceptance rates.

Most of this information is available in our databases (and is partially collated in the membership slides). To determine exact data for the membership, a representative date is required for which the (membership) statistics are computed. After a discussion the first of September is chosen as the best date to report on the composition of IACR's membership.

Action Point **19: Cachin, shelat, Smart** *(1 June 2013)*: Determine which information and statistics IACR should publish online and where.

10.2. ***Eurocrypt'15.*** Dimitar Jetchev, Svetla Nikova, and Georgi Sharkov present a proposal to host *Eurocrypt 2015* in Sofia, Bulgaria, tentatively in the last week of April. There is some discussion on the budget and the possibility to increase the budget to encourage local participation.

The Board unanimously accepts the proposal.

Decision 7. *Eurocrypt 2015 will be held in Sofia (Bulgaria) and Svetla Nikova and Dimitar Jetchev are appointed General co-Chairs. [with Nikova serving on the IACR Board.]*

11. Conference Chairs

11.1. **Program Chairs Reports.** Benaloh feels there is not a lot to report.

Action Point **20: Benaloh** *(no time set)*: Chase program chairs for reports

11.2. **Program and General Chair List Maintenance.** 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.

shelat (obo Lysyanskaya) remarks on the gender (im)balance on the lists and calls for an increased bias to benefit people running for tenure.

11.3. **Crypto'14–'15.** Juan Garay has already been appointed as one of the co-chairs for *Crypto'14*. Several excellent candidates are nominated, and after discussion a candidate is selected.

Decision 8. *Rosario Gennaro is appointed Program Chair (rolling co-chair) for Crypto'14 and Crypto'15. [Gennaro subsequently accepted.]*

11.4. **Asiacrypt'14–'15.** Preneel very quickly explains the procedure and notices that for *Asiacrypt'14* Palash Sarkar has already been appointed as one of the co-chairs. Several excellent candidates are nominated, and after discussion a candidate is selected.

Decision 9. *Tetsu Iwata is appointed Program Chair (rolling co-chair) for Asiacrypt'14 and Asiacrypt'15. [Iwata subsequently accepted.]*

12. Strategy

12.1. **ICT Infrastructure and IACR Publications.** In January the contract with Springer has been signed. The contract is for 4 years, which means that by *Eurocrypt'15* a plan needs to be in place for what happens afterwards. Everything pre-2000 is owned by Springer, but it is currently open access courtesy of Springer. From 2000–2008 it is open for now on Springer, and IACR has slightly different versions in its archive. For the period 2008–2012 the situation is slightly more complex, but the IACR will gradually be able to make its version publicly available on the archive. For publications from 2013, open access of the Springer version is guaranteed with an (open access) publication delay of 4 years.

Preneel explains the new copyright form, which defines the different versions, the mandated or suggested footnotes, and the emphasis on the DOI for identification of papers. For illustrations and theses there are standard exceptions included in both the contract with Springer and the copyright form that allow reuse by the authors without worrying about copyright. A new part of the form is used to ask authors for licensing IACR to distribute slides, presentations, and possibly tools and implementations. Several exceptions are discussed, some of which still need some verification.

Authors may put an author's version on eprint immediately and IACR may make indexed IACR versions available publicly after two years. To not make an already complicated situation even more complicated, IACR should endeavour that the author's version can serve as IACR version. Authors have the right to modify their version to mimick the Springer version apart from a different mandated footnote. The workflow to ensure the author's version is contract-compliant will be quite complicated. For instance, the mandated footnote requires a DOI, which is not obvious as the DOI will only be available after formal publication. To coordinate and check that the right files are available at the right place at the right time, the IACR will likely need a publication officer taking responsibility. Orman has most experience so far given her experience with the archive.

Smart has created a preliminary proposal workflow based on applying relatively minor modifications to the current IT infrastructure. Cachin suggests to make the new flow available on our website.

The question is raised whether the IACR will allow author's versions of non-IACR papers on the eprint archive. Smart explains why this is beneficial and he suggests a change in the wording of eprint's terms, therebye allowing author's version even from other cryptology conferences. The Board agrees that this is a good idea.

Action Point **21: Cachin and Smart** *(no time set)*:
Establish a new policy for the IACR eprint to enable green open-access versions of non-IACR publications.

The discussion moves to a strategic, long term publishing solution. There is a consensus that printing on paper is no longer an important part of the publication process, but providing open access and ensuring a high scientific standard are. The current, rolling model with Springer only provides a constrained form of open access.

Preneel notices that in Nature there recently was an issue on open access publications. If the IACR is to change its publication model, the Board would have to put forward a concrete proposal to the membership. To facilitate discussion at a membership meeting, ideally the slides for such a proposal are available as part of the Crypto delegate pack. A formal decision would have to be made by Crypto 2014 in order to leave enough time for negotiation and implementation.

Smart explains two different journference models. These would lend themselves to a gradual transition which might also help smooth ISI indexing. A discussion ensues that highlights the diversity of opinions on this important topic.

- Abdalla does not see a lot of problems with the current system.
- Leander would like to improve the refereeing process and the quality of publications. This refers in part to how much of a paper is reviewed (avoiding multiple reviewing of a subpart of a paper) and where a full version is actually published. He suggests a postproceedings system. Since properly reviewing a paper is a significant investment, he also wonders what scientific credits should be attached to reviewing.
- Lin notices that there is a problem who accepted journference papers get assigned to a conference: as there are three annual IACR conferences (as opposed to only one for some other fields that moved to a journference model) the reviewing process might not guarantee that a submission will be accepted in time for a particular conference deadline.
- Smart prefers a model where more papers are published than presented, where presentations are a badge of honour. Cachin believes that this badge would create more complications.

Other communities encountered similar problems and came up with various other solutions (and IACR might be able to partner with Usenix as part of a publishing solution). To facilitate discussion during the membership meeting, Smart will give a presentation to highlight perceived problems and a possible solution during the rump session.

Action Point **22: Smart** *(27 May 2013)*:
Create slides that reflect current Board thinking on the problems of the current publication model and suggest possible radical solutions.

12.2. **Program Balance at IACR Flagship Conferences.** There is no discussion on this issue this Board meeting.

13. Closing Matters

13.1. **Draft Agenda for General Meeting of Members.** Preneel quickly recapitulates the main issues to discuss at the membership meeting. There is a brief discussion about preparing to an opt-in model for the Journal of Cryptology, in particular the effect it would have on the membership fee.

13.2. **Review of Action Items.** After a brief review of action points, Preneel closes the meeting at 19.00.

14. Intermediate Board Decisions

Decision 10. *The Board approves the FSE'14 proposal, meaning that FSE 2014 will be held in London (UK) with Christian Rechberger and Carlos Cid as as General and Program co-Chairs.*

Decision 11. *Josh Benaloh and Tom Berson are appointed to the Ethics Committee for the 2013 calendar year. (As Vice President, Christian Cachin is automatic member and chair of the Ethics Committee.)*