MINUTES IACR BOARD MEETING *EUROCRYPT'11*

1. Opening

At 10.06 Preneel opens the meeting. 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 original agenda for consistency. There was an adjournment for lunch from 13.15 to 14.08.

1.1. Roll of Attendees.

There are 17 attendees, holding a further 5 proxies.

Attendees (Elected). Josh Benaloh (Director –2011); Christian Cachin (Vice-President –2013); Antoine Joux (Director –2011); Matsuru Matsui (Director –2013); Christof Paar (Director –2013); David Pointcheval (Director –2013, PKC Steering Committee); Bart Preneel (President –2013, FSE Steering Committee); Greg Rose (Treasurer –2013); Martijn Stam (Secretary –2013); Serge Vaudenay (Director –2012).

Attendees (Appointed). Shai Halevi (Membership Secretary –2011); Hyoung-Joong Kim (GC *Asiacrypt'11*); Helger Lipmaa (GC *Eurocrypt'11*); Nigel Smart (GC *Eurocrypt'12*); Christopher Wolf (Newsletter Editor –2012).

Attendees (Representatives and Others). Tsutomu Matsumoto (Asiacrypt Steering Committee); Jean-Jacques Quisquater (CHES Steering Committee); Aggelos Kiayias (for Point 10.1 only).

Absentees (Elected). Tom Berson (Director –2012, proxy Cachin); Stuart Haber (Director –2011, proxy Benaloh); David Nacchache (Director –2012, proxy Pointcheval).

Absentees (Appointed). Matt Franklin (Journal Editor-in-Chief –2011, no proxy); Xuejia Lai (GC *Asiacrypt'12*, no proxy); Tom Shrimpton (GC *Crypto'11*, proxy Cachin); Yiqun Lisa Yin (GC *Crypto'12*, proxy Halevi).

Absentees (Representatives and Others). Ivan Damgård (TCC Steering Committee); Kevin McCurley (Database Administrator); Hilarie Orman (Archivist).

1.2. Action Points.

Preneel briefly reviews the status of action items identified from the Crypto'10 meeting.

1.3. *Eurocrypt'11* Status.

Lipmaa (GC *EC'11*) mentions the major problems that the organization of *Eurocrypt'11* has encountered so far:

- The break even went from 460 USD to 500 USD (the original budget was at a rate of 1 EUR = 1.25 USD, which has changed to 1 EUR = 1.48 USD).
- Fewer people ($\approx$ 300) have registered than was foreseen ($\approx$ 360). As a result a larger percentage of the registration fee will have to be used to cover fixed costs. On a positive note, 21 people from the Estonian community have registered so far.

Small cuts have been put in place to mitigate the effect of the reduced income. The Board emphasizes that IACR guarantees currency fluctuations so that this should not be a worry for the organizing committee.

2. Officer's Report for Approval

2.1. Treasurer's Report.

Rose mentions that *Crypto'10* is projected to make a profit. The general financial situation of the IACR is healthy, but the current asset spread is not ideal. Alternatives are discussed and the Board asks Rose to put these forward to the Assembly.

3. Guidelines for Approval

3.1. Program Chair Guidelines.

Date: Talinn, 12 May 2011.

Rolling co-chairs. Cachin explains the proposed changes to the guidelines. Preneel thanks Christian for his work incorporating the rolling co-chair model into the (draft) guidelines.

The Board discusses the pros and cons of the rolling co-chair model for the flagship conferences (Eurocrypt, Crypto, Asiacrypt; for the workshops the steering committees are responsible) and what possible alternatives could look like. Several past program chairs have indicated that being a chair is hard work and that the experience often leaves them with ideas how to chair, but no opportunity to implement these. This feedback was part of the motivation to to introduce the rolling co-chair model. While the co-chair system was nominally already in place for *Eurocrypt'11* and *Crypto'11*, the 'junior' chair had only limited involvement, partly due to unclarity of the system.

A comparison is being made with other conferences with a co-chair system. For the 'Oakland' conference, the two (rolling) co-chairs really share the work 50-50 (source: Wagner); CHES has always had (non-rolling) co-chairs, where the steering committee asks one person first and whether (s)he would be willing to cochair with the other. There are no senior–junior problems.

The Board feels that having a co-chair system is beneficial and discusses how to implement the system: formally as rolling co-chairs (in the guidelines) or informally (where the Board would as a tradition reappoint the junior chair for a second year). There is consensus that the formal approach provides most clarity (and still leaves the Board the option to intervene if needed).

Decision 1. *The rolling co-chair model as outlined in the draft guidelines is accepted.*

Action Point **1: Christian Cachin** *(Asap [since completed])*:
Finalize the new Program Chair Guidelines.

Transition regime. One of the consequences of the rolling co-chair model is that the second co-chair needs to be appointed sooner than would currently be the case (as preparations such as appointing a program committee take place roughly 18 months in advance, whereas previously chairs were appointed two years in advance of their 'senior' conference, which is only a year before their 'junior' conference). This means that in future the Board will need to appoint

- the *Eurocrypt'*$(x+2)$–'$(x+3)$ program chair at *Crypto'*x (this results in a decoupling with the decision where to host the conference: *Eurocrypt'*$(x+2)$ would have been taken at *Eurocrypt'*x; *Eurocrypt'*$(x+3)$ will only be decided at *Eurocrypt'*$(x+1)$).
- the *Crypto'*$(x+1)$–'$(x+2)$ program chair at *Eurocrypt'*x;
- the *Asiacrypt'*$(x+1)$–'$(x+2)$ program chair at *Eurocrypt'*x, or *Crypto'*x at the latest (here no decoupling is desired, so the hosting of *Asiacrypt'*$(x+2)$ will be taken in conjunction).

In particular, at the present meeting the Board will need to decide on the *Crypto'12–'13* program chair (in addition to the already scheduled *Eurocrypt'12–'13* program chair). At the upcoming Board meeting at *Crypto'11*, the decisions for the *Asiacrypt'12–'13* and *Eurocrypt'13–'14* program chairs will need to be made.

Cachin notices that other guidelines (general chair, ethics) need to be updated as well and suggests setting up a wiki/svn for this on the server.

4. Appointees Reports for Information

4.1. **Membership Secretary Report.** Halevi briefly reports and notices that IACR membership has stabilized (i.e. is no longer increasing).

4.2. **JoC Editor in Chief.** On behalf of the EiC (Matt Franklin), Preneel reports that everything is on track. The Board has a discussion about some of shortcomings of the current (non-automated) system, such as the difficulty to keep track of what is currently in the pipeline. A web-based system might be more suitable and while the EiC is best placed to figure out the requirements of such a system, others might be of assistance figuring out the best system to meet these requirements.

Action Point **2: Nigel Smart, Shai Halevi, Matt Franklin** *(Week before Crypto'11)*:
Investigate the requirements of a possible web-based system and examine if existing solutions match these requirements and (if not) what building (and maintaining) a satisfactory system would cost. Report back the week before *Crypto'11* with the objective to have the system implemented at the end of the calendar year.

4.3. **Archivist.** On behalf of the Archivist (Hilarie Orman), Preneel indicates that there is a lack of communication.

4.4. **Newsletter.** Wolf gives an update on the Newsletter.

5. Internal Committee Reports for Information

5.1. **Fellows Committee.** The Fellows Committee is in need of more nominations. It is pointed out that the Fellows Committee itself can also nominate members and that previously it was decided that fellows ought to be members for life.

5.2. **Electronic Publishing Committee.** Preneel mentions that in the next months an opt-out system will be implemented for the mailing of paper copies of the Journal of Cryptology.

5.3. **Ethics Committee.** Cachin mentions that the new guidelines are about to be published but still need some further alignment.

Action Point **3: Christian Cachin** *(Before Crypto [since completed])*:
Make a proposal for the ethics guidelines and send it around

Decision 2. *Jean-Jacques Quisquater and Serge Vaudenay are appointed to the Ethics Committee. (As Vice President, Christian Cachin is automatic member and chair of the Ethics Committee.)*

6. Appointments

6.1. **Election Committee.**

Decision 3. *Greg Rose, Serge Vaudenay, and Martijn Stam are appointed to the Election Committee for the 2011 election.*

7. Conferences since last BoD Meeting

7.1. ***Crypto'10.*** The conference was well-organized and the collocation (with *CHES'10*) a success. A small profit was made.

7.2. ***Asiacrypt'10.*** The general chair could not make it, Matsumoto reports. The conference had around 240 attendees from around the world and made a substantial profit. Overall it was an excellent and well-organized event.

8. Forthcoming Conferences for Information

8.1. ***Crypto'11.*** All is going well.

8.2. ***Asiacrypt'11.*** Kim (GC *AC'11*) gives an update. Financially, more accurate hotel prices are reported, as well as an impressive amount of sponsoring. Kim mentions some fresh ideas, for instance the guided tour will likely be on the Monday afternoon.

8.3. ***Eurocrypt'12.*** Smart (GC *EC'12*) gives an update. Sponsoring is going well. For the housing around 200 college rooms will be available. The conference venue will be able to hold 400 to 500 people.

8.4. ***Asiacrypt'12.*** Matsumoto reports that all is going well (including sponsoring).

9. Steering Committee Reports and Workshop Proposals

9.1. **Asiacrypt.** Matsumoto will continue as chair of the Asiacrypt Steering Committee; the next meeting is scheduled for *Crypto'11*.

9.2. **TCC.** *TCC'11* went well. *TCC'12* was originally planned for Japan, but due to the recent events, the TCC Steering Committee suggests to move to Taormina instead. The proposal is solid and the Board approves.

Decision 4. *The Board approves the TCC'12 proposal, meaning that TCC 2012 will be held in Taormina (Italy) with Nelly Fazio and Rosario Gennaro as General co-Chairs, Dario Catalano as the local arrangement chair, and Ronald Cramer as Program Chair.*

9.3. **PKC.** Pointcheval reports that *PKC'11* went well and had 80 participants. *PKC'12* was originally planned for Japan, but the steering committee is discussing with the local organizers whether a move would be prudent. The Board emphasizes that any cancellations costs can be born by the IACR, but that otherwise the decision is mainly up to steering committee. [The PKC Steering Committee subsequently sent round a proposal for *PKC'12* to be held in Darmstadt, which was approved by the Board.]

9.4. **FSE.** Preneel reports that with around 150 participants, *FSE'11* was well attended. *FSE'12* is likely to be collocated with the final NIST SHA-3 workshop, with proposed general chair Bruce Schneier and program chair Anne Canteaut. A more detailed proposal is forthcoming. [The FSE Steering Committee subsequently sent round a proposal for *FSE'12* to be held in Washington D.C., which was approved by the Board.]

9.5. **CHES.** The collocation of *CHES'10* with *Crypto'10* was a real success, both in terms of the overall number of attendees and the programmatic overlap. *CHES'11* has been moved at late notice from Tokyo to Nara (Japan). The local organizers are thanked for their quick response under difficult circumstances. The steering committee so far has received two proposals for *CHES'12*.

10. Conference Proposals for Discussion/Selection

10.1. ***Eurocrypt 2013.*** Aggelos Kiayias gives a well-received presentation about the bid to hold *Eurocrypt 2013* in Athens, Greece. After some questions and discussion, the Board recommends to explore the possibility of holding the event mid-April (to cut costs). The Board unanimously approves the proposal and thanks Aggelos and his team for an excellent proposal.

Decision 5. *Eurocrypt 2013 will be held in Athens (Greece) and Aggelos Kiayias is appointed General Chair. [Aggelos Kiayias subsequently accepted.]*

Action Point **4: Greg Rose** *(Asap)*:
Update the GC guidelines and the spreadsheet with respect to the IACR fee.

10.2. ***Asiacrypt 2013.*** Matsumoto mentions that the Asiacrypt steering committee had received two proposals and that it has unanimously chosen the proposal from the United Arab Emirates (UAE). It is noted that the financial health of the proposal hinges on a large amount of sponsorship. The Board wonders whether recent developments might have changed the likelyhood of procuring this sponsorship and/or the interest of a potential General Chair to organize *Asiacrypt 2013*. Clarification on some other points is also felt desirable.

Action Point **5: Matsumoto** *(Before Crypto)*:
Inform whether the Steering Committee can resolve the issues brought up by the Board with the local organization.

11. Conference Chairs

11.1. **Program Chair Reports.** Joux explains his *FSE'11* report. He notices that nothing special has happened, although there were complaints about the PC balance after the fact (he did try to increase gender balance).

The *TCC'11* report is briefly discussed; nothing seemed out of the ordinary.

11.2. **Program and General Chair List Maintenance.** Stam justifies some of the recent maintenance and asks for further suggestions. The received suggestions will be incorporated for next Board meeting.

11.3. **Eurocrypt'12–'13 Program Chair.** Preneel and Benaloh explain the procedure, but some shortcomings are encountered. It is emphasized that we are appointing within the rolling co-chair model, and Pointcheval (the already appointed co-chair for *Eurocrypt'12*) confirms his intention to make the model work. Several excellent candidates were nominated, and after discussion a candidate was selected.

Decision 6. *Thomas Johansson is appointed Program Chair (rolling co-chair) for Eurocrypt'12 and Eurocrypt'13. [Thomas Johansson subsequently accepted.]*

Action Point **6: Josh Benaloh** *(Before Crypto)*:
Update the internal voting protocol.

11.4. **Crypto'12–'13 Program Chair.** This appointment was not originally on the agenda, but is brought forward in light of the rolling co-chair model. Rei Safavi-Naini (the already appointed co-chair for *Crypto'12*) is not present at the meeting, but Preneel will brief her on what was decided during this Board meeting. Several excellent candidates were nominated, and after discussion a candidate was selected.

Decision 7. *Ran Canetti is appointed Program Chair (rolling co-chair) for Crypto'12 and Crypto'13. [Ran Canetti subsequently accepted.]*

11.5. **Asiacrypt'12–'13 Program Chair.** This appointment is postponed until *Crypto'11*.

12. Strategy

12.1. **Website Redesign.** Wolf opens the discussion with a short presentation. While the website has its fair share of visitors, it looks somewhat outdated. Moreover, the current system evolved over the years and has various components and technologies that are not integrated very well. It is recognized that taking the website to the next level (and maintaining it) will likely cost money, even when using open source tools. Currently it is not clear exactly what the options are and what they would cost.

> Action Point **7: Christian Cachin, Christopher Wolf, Shai Halevi, Kevin McCurley** *(Crypto'11 BoD)*:
> Present a concrete proposal regarding the future of the IACR website.

Wolf mentions that over the past period, he has hired a student on IACR's behalf to maintain and improve the website (resulting in e.g. the PhD-database). He wishes to continue this collaboration and requests appropriate funds for this. This request is met with approval.

Decision 8. *The Website manager is given permission to hire (from IACR means) a student for half a year.*

12.2. **Electronic Voting Update.** Benaloh reports on the experiences of the November'10 elections using electronic voting.

(1) It turned out that the period of the election was unreasonably long: the vast majority of votes came in either at the beginning or at the end (after a reminder). A period of four weeks (from Oct 15–Nov 15) would be sufficient (and create some distance from Crypto). However, the election period is mandated by the bylaws, so implementation of this change will have to wait until the next time we change the bylaws.
(2) Some people were confused about their membership and who is a member when.
(3) The current system uses aliases instead of names for voters. An alternative would be to link the names of voters to encrypted ballots. This would publicly show who has engaged in the election and who has not (currently it is hidden). In the ensuing discussion no consensus was found as to whether this would be a good or a bad thing. The Assembly will be asked for an opinion.
(4) Benaloh suggest to move to full approval voting for the Directors. Currently each member can only vote for at most three Directors on the ballot and the three Directors with the most votes are chosen. For full approval voting, a member can vote for as many Directors as desired; as before the three Directors amassing most votes are elected. Full approval voting tends to give a better representation. Although the change can be implemented without a need to touch the bylaws, it would require updating of the software used.

Decision 9. *The IACR Election for Directors will henceforth be conducted using full approval voting.*

Decision 10. *IACR will support Helios to implement full approval voting (preferably by October this year) by a donation of 1000 USD.*

12.3. **IACR Publication Strategy.** Preneel presents several possible changes to the current publication strategy. One option that is discussed is to offer the membership with or without paper copy of JoC, but this would require further thinking and most likely a bylaws change. Preneel will talk to Kevin McCurley and Stuart Haber and hopes to present more concrete plans at Crypto'11.

12.4. **Future Scheduling of Workshops.** In 2010 there were two IACR Workshops collocated with a Conference: PKC took place in Paris just before Eurocrypt took place in the French Rivièra and CHES and Crypto took place back to back with some interleaving (both at UCSB). Bart Preneel reports this worked well and the Board agrees. Future collocation should be encouraged, bearing in mind that scheduling of the workshops is primarily the domain of the respective steering committees. One possibility would be a rolling collocation model for PKC/FSE/TCC with Eurocrypt, and possibly CHES collocated with Crypto once every three years. Collocation with Asiacrypt might be harder to schedule. Collocation with other events is fine as long as there are no formal proceedings, to prevent competition with IACR's event(s).

> Action Point **8: SC representatives** *(before Crypto)*:
> Ask the respective steering committees for an opinion about increased collocation.

12.5. **Request for Sponsorship.** Preneel provides some background information on the request. While it would be money well-spent, it is felt that it would be inappropriate to honour the request.

13. Closing Matters

Joux announces this was his last Board meeting, as he will not attend *Crypto'11* and does not intend to run again.

A draft agenda for the general meeting of members is briefly discussed. For evoting a straw poll for displaying who has voted will be held; the switch to approval voting has to be announced. Related to publishing, some further attention will be drawn to the online archive. An update about IACR's future publishing strategy will be given, with the remark that not having proceedings at FSE (the general chair's prerogative) seemed to work out fine. (A review of the membership fee will be later.)

After a brief review of action points, Preneel closes the meeting at 17.40.

14. Intermediate Board Decisions

Decision 11 (20 June 2011)**.** *The Board approves the PKC'12 proposal, meaning that PKC 2012 will be held in Darmstadt (Germany) with Johannes Buchmann as General Chair, Mark Manulis as General co-Chair, and Marc Fischlin as Program Chair.*

Decision 12 (4 August 2011)**.** *The Board approves the FSE'12 proposal, meaning that FSE 2012 will be held in Washington D.C. (USA) with Bruce Schneier as General Chair and Anne Canteaut as Program Chair.*