MINUTES IACR BOARD MEETING *EUROCRYPT'12*

CAMBRIDGE (UK), 11 APRIL 2012

1. Opening Matters

At 10.03 Preneel opens the meeting and he mentions that some people might arrive a bit later. 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 around noon.

1.1. **Roll of Attendees.** There are 20 attendees, holding a further 3 proxies.

Attendees (Elected). Josh Benaloh (Director –2014); Tom Berson (Director –2012); Christian Cachin (Vice-President –2013); Shai Halevi (Director –2014); Mitsuru Matsui (Director –2013); David Nacchache (Director –2012); David Pointcheval (Director –2013, PKC Steering Committee); Bart Preneel (President –2013, FSE Steering Committee); Greg Rose (Treasurer –2013); Nigel Smart (Director –14, GC *Eurocrypt'12*); Martijn Stam (Secretary –2013); Serge Vaudenay (Director –2012).

Attendees (Appointed). Matt Franklin (Journal Editor-in-Chief –2014); Aggelos Kiayias (GC *Eurocrypt'13*, for Agenda Item 7.3 only); Xuejia Lai (GC *Asiacrypt'12*); Satya Lokam (GC *Asiacrypt'13*); Christopher Wolf (Newsletter Editor –2012).

Attendees (Representatives and Others). Kevin McCurley (Database Administrator); Jean-Jacques Quisquater (CHES Steering Committee).

Absentees (Elected). Christof Paar (Director –2013, proxy Wolf);

Absentees (Appointed). abhi shelat (Membership Secretary –2014, proxy Halevi); Helena Handschuh (GC *Crypto'13*, proxy Preneel); Yiqun Lisa Yin (GC *Crypto'12*, proxy Rose).

Absentees (Representatives and Others). Ivan Damgård (TCC Steering Committee, proxy Halevi); Tsutomu Matsumoto (Asiacrypt Steering Committee, proxy Matsui); Hilarie Orman (Archivist).

1.2. **Minutes.** The minutes of the BoD meeting at *Crypto'11* and the membership meetings of *Eurocrypt'11* and *Crypto'11* are approved with some minor changes. Wolf requests a change in the layout so that Board decisions stand out more. [Cachin later requested a more prominent display of the date.]

1.3. **Action Points.** Preneel briefly reviews the status of action items identified from the *Crypto'11* meeting.

(1) (Election documentation) Benaloh rolls this forward to *Crypto'12*.

> Action Point **1: Josh Benaloh** *(1 August 2012)*:
> Update Board voting guidelines and provide Helios election guidelines.

(2) (IACR Website and ICT) A lot of work has been made and the website looks a lot better as a result. Preneel takes the opportunity to thank the team responsible. Cachin and McCurley mention that the process is still ongoing and in need of further volunteers.

> Action Point **2: Preneel** *(1 August 2012)*:
> Find more volunteers to help with the web.

(3) (Reserve diversification) Postponed to Agenda Item 2.1.
(4) (Guidelines update) Postponed to Agenda Item 4.3.
(5) (Guidelines incorporation) Halevi rolls this forward to *Crypto'12*.

> Action Point **3: Shai Halevi** *(1 August 2012)*:
> Integrate a link to the relevant ethics guidelines in the review website.

(6) (Copyright archiving) McCurley has discussed with Orman about a different web-based interface. He is planning a further conference call to discuss. It should be put in the bylaws that the Secretary is responsible for the archiving of copyright forms.
(7) (JoC software discussion) Smart mentions that he modified a big system to make it compatible with our current work flow. One problem is an unclarity where to host this system. Complications arise as such a system is not a fixed object; patches to the original (e.g. security related) would need to be incorporated to the modified system. With other available systems the EiC is typically more omnipotent than desired for the IACR JoC. There is currently no good solution.

> Action Point **4: Smart, Franklin, McCurley** *(no time set)*:
> Try to find a working solution for a web-interface for the JoC reviewing process.

(8) (Successor Membership Secretary) abhi shelat has been appointed.

1.4. ***Eurocrypt'12* Status.** Smart (GC *EC'12*) says that there are about 400 delegates and that all the rooms in Robinson college have been sold, thereby removing the risk that was initially taken. He mentions that he is relatively relaxed about the conference. There will again be videos of the talks, but with a slight difference compared to last year's Crypto (with more emphasis on the slides and less on video of the speaker).

McCurley mentions that he has spent a lot of work for *Crypto'11* and recommends that the system to capture and edit videos changes to one that requires less postprocessing on his (or IACR's) behalf.

Preneel thanks Smart and McCurley for their work.

2. Officer's Report for Approval

2.1. **Treasurer's Report.** Rose mentions he has done a large amount of exploration about diversification. It turns out to be harder than he originally thought. A board resolution, signed by the Officers, is needed to proceed. After deliberation, the Board decides to proceed, noting that a further board decision is needed before actual diversification would be implemented.

Decision 1. *On behalf of the IACR, the Treasurer (Greg Rose) is authorized to start negotiations with banks regarding diversification of the IACR reserve.*

> Action Point **5: Greg Rose** *(before Crypto'12)*:
> Get a signed board resolution for exploration and present a concrete proposal

Rose points out that there is a California law stipulating that if the turnover is above a certain threshold, then an audit is required. With the registrations of the events all going through the central IACR servers, the turnover is getting dangerously close to this threshold.

Berson suggests to create an audit committee that is responsible for ensuring proper audits. This committee would need at least two board members and a majority of non-board members. Previous treasurers are mentioned as obvious candidates.

> Action Point **6: Tom Berson** *(at Crypto'12)*:
> Propose an audit committee.

Rose notices that IACR recently is getting a lot more sponsorship for its events.

Preneel has been approached by Google to have a recurring student sponsorship. McCurley mentions that additionally there is a separate program by Google for women.

There is a brief round of applause for the current sponsors.

3. Appointees Reports for Information

3.1. **Newsletter.** Wolf mentions that business is as usual, although the change of the system has taken some time. Chairs (of IACR events) are also capable of sending news. Preneel thanks Wolf for doing an excellent job.

3.2. **JoC Editor in Chief.** Franklin says everything is going smoothly and all is looking good.

3.3. **Membership Secretary.** Preneel (obo shelat) says he is on top of things. Membership level is still stable.

3.4. **Archivist.** Preneel (obo Orman) says that she has been active discussing copyright forms etc. McCurley says there are still integrating pieces to keep up. The focus seems to be based on LaTeX and less on metadata.

3.5. **Database.** McCurley says that there are several databases on the IACR server that are not integrated very well at all. It would be beneficial to increase or improve mutual integration, but unification would require a unified authentication system. There is a discussion on how best to proceed.

Preneel thanks the team (McCurley, Franklin, Wolf, Orman) responsible.

4. Internal Committee Reports for Information

4.1. **Fellows Committee.** Preneel (obo Maurer) reports that the Fellows committee have appointed several new fellows, namely Mihir Bellare, Eli Biham, Manuel Blum, Andrew Odlyzko, Phil Rogaway, Claus Schnorr, and Jennifer Seberry. Of these new fellows, Biham, Rogaway, and Seberry have chosen to be inducted during *Eurocrypt'12*; the remaining four will join during *Crypto'12*.

The new chair for the Fellows committee will be Arjen Lenstra.

4.2. **Electronic Publishing Committee.** To be discussed later.

4.3. **Ethics Committee.** Cachin reports that no complaints have been received yet. Given the one-year tenure of the committee, he proposes to reappoint the committee.

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.)*

> Action Point **7: Martijn Stam** *(no time set)*:
> Keep better track of all the various committees

4.4. **JoC web system evaluation.** This point has already been discussed (during the Action Points, Section 1.3).

5. Appointments

5.1. **Election Committee.**

Decision 3. *Josh Benaloh, David Pointcheval, and Greg Rose are appointed to the Election Committee for the 2012 election.*

5.2. **Newsletter Editor.** The current appointment of Wolf as Newsletter Editor will end before *Crypto'12*. Preneel thanks Wolf for his efforts and proposes to reappoint him. This is unanimously accepted.

Decision 4. *Christopher Wolf is appointed Newsletter Editor for the period 2012–2014.*

6. Conferences since last BoD Meeting

6.1. ***Crypto'11.*** Preneel (obo Shrimpton) reports that concluding affairs for *Crypto'11* has been successful.

6.2. ***Asiacrypt'11.*** Matsui (obo Kim) says that everything went well and there is nothing extraoardinary to report.

7. Forthcoming Conferences for Information

7.1. ***Crypto'12.*** Rose (obo Yin) reports all is going well. She is in discussion with the Program co-Chairs (Canetti and Safavi-Naini) about increasing the space for parallel talks and possibly a tutorial on Sunday. Thanks to successful sponsoring acquisition the registration fee might be brought down slightly.

Preneel thanks Yin for doing an excellent job.

7.2. ***Asiacrypt'12.*** Lai reports on the progress. The submission deadline is next month. Finances are still a bit subject to fluctuation. The venue has moved to the former site of the Beijing Olympics. Preneel thanks Lai for doing an excellent job.

7.3. ***Eurocrypt'13.*** Kiayias (GC *EC'13*) gives an update. The dates have been fixed to 26 to 30 May 2013. The hotel contract has been signed and prices have been negotiated down. There is potential for the conference room to be split in two for parallel sessions if necessary. Preneel thanks Kiayias for doing an excellent job.

8. Steering Committee Reports and Workshop Proposals

8.1. **Asiacrypt.** Matsui (obo Matsumoto) says that there is nothing to report beyond the separate relevant items on the agenda.

8.2. **TCC.** Halevi (obo Damgård) mentions the reports by Goldreich (*TCC* SC chair) and Damgård and has nothing to add.

8.3. **PKC.** Pointcheval says there was a record number of submissions for the upcoming *PKC'12* in Darmstadt and a large number of participants is expected.

Next year, *PKC'13* will be in Nara. There is some possibility that in 2014 PKC will be held in Argentina.

Cachin brings up the PKC website, which once existed but has since disappeared. It would be good if the PKC steering committee made its rules and composition publicly available. IACR can host a website if content is delivered by the steering committee.

8.4. **FSE.** Preneel gives some background to the report. *FSE'12* went well, Schneier (*FSE'12* GC) and Canteaut (*FSE'12* PC) did a good job. There were around 140 participants from all over the globe.

8.5. **CHES.** Quisquater gives a brief presentation on *CHES'11* that took place in Nara, Japan. *CHES'12* will be in Leuven. There is no recent news; everything seems to be on track.

He also presents a proposal for *CHES'13*, to be colocated with *Crypto'13*. The proposal is approved, with the remark that the budget is still missing and will have to be submitted for approval prior to Crypto'12.

Decision 5. *The Board approves the CHES'13 proposal, meaning that CHES 2013 will be held in Santa Barbara (USA), colocated with Crypto 2013. Çetin Kaya Koç and Thomas Eisenbarth are appointed General co-Chairs and Guido Bertoni and Jean-Sébastien Coron are appointed Programme co-Chairs.*

9. Conference Proposals for Discussion/Selection

9.1. **Asiacrypt 2013.** Preneel recapitulates the history of the *Asiacrypt 2013* proposal. After the problems with the UAE proposal, the AC SC has approved a proposal from Bangalore.

Satya Lokam joins the meeting and gives a presentation about the proposed *AC'13*. The Board asks several questions to assess the bid, focussing on the proposed venue and the transportation. The AC SC is supportive of the proposal. The Board unanimously votes in favour and expressses a strong preference for a central location. Satya Lokam accepted and attended the rest of the meeting as appointed board member.

Decision 6. *Asiacrypt 2013 will be held in Bangalore (India) and Satya Lokam is appointed General Chair.*

9.2. **Eurocrypt 2014.** Lars Knudsen and Gregor Leander join the meeting for this point and give a wonderful presentation about the possibility to host Eurocrypt in Copenhagen in 2014. After some questions from the board, Preneel thanks Leander and Knudsen for their work in preparing the proposal. Lars will be the vice-chair. The Board unanimously votes in favour and encourage the chairs to try to bring down the registration fees (possibly by taking some more risks).

Decision 7. *Eurocrypt 2014 will be held in Copenhagen (Denmark) and Gregor Leander and Lars Knudsen are appointed General co-Chairs. [Gregor Leander and Lars Knudsen subsequently accepted, with the understanding that Gregor Leander will serve on the IACR Board of Directors as Eurocrypt 2014 General Chair.]*

9.3. **Asiacrypt 2014.** DJ Guan gives a good presentation and briefly addresses visa issues with China. After some questions, Preneel thanks Guan for his excellent proposal. The AC SC gives some background information. The Board unanimously votes in favour.

Decision 8. *Asiacrypt 2014 will be held in Kaohsiung (Taiwan) and DJ Guan is appointed General Chair. [DJ Guan subsequently accepted.]*

> Action Point **8: Greg Rose** *(no time set)*:
> Sort out the template to deal better with student stipends and free attendees

10. Conference Chairs

10.1. **Program Chairs Reports.** Benaloh reports he did not receive many reports; no special issues were mentioned in those he received. He also indicates having some issues with initial contacts.

10.2. **List Maintenance.** There are some additions to and removals from the lists.

10.3. **Asiacrypt'13–'14.** Preneel very quickly explains the procedure and notices that for *Asiacrypt'13* Kazue Sako has already been appointed as one of the co-chairs. Several excellent candidates are nominated, and after discussion a candidate is selected.

Decision 9. *Palash Sarkar is appointed Program Chair (rolling co-chair) for Asiacrypt'13 and Asiacrypt'14. [Sarkar subsequently accepted.]*

10.4. **Crypto'13–'14.** Ran Canetti has already been appointed as one of the co-chairs for *Crypto'13*. Several excellent candidates are nominated, and after discussion a candidate is selected.

Decision 10. *Juan Garay is appointed Program Chair (rolling co-chair) for Crypto'13 and Crypto'14. [Garay subsequently accepted.]*

11. Strategy

11.1. **Website redesign.** The redesign has already been discussed.

11.2. **Future scheduling of workshops.** The steering committees are reminded of the potential.

11.3. **Electronic voting update.** Vaudenay presents his report. The election might have looked relatively smooth from the outside, but there were a fair bit of problems behind the scenes. Thanks to Ben Adida all bugs were repaired in time. Nonetheless, the robustness of the process seems to rely heavily on a single person.

Preneel mentions that we should test Helios better.

11.4. **IACR Publication Strategy.** Preneel discusses the goals of IACR and how its publication strategy meets these goals. IACR has been conservative so far and making major changes carries a reputational risk. He mentions that the rolling contract with Springer will expire at the end of this year. Several possible options are presented. Preneel notices that the decision ideally has to be made before the Calls for Papers of the early conferences, which means July/August at the latest.

There is extensive discussion to cut down the possible solutions, with an emphasis on what the most important criteria are. McCurley claims that reputation is the hardest to compromise on, as a lot of decisions important to the IACR membership (e.g. promotions, grant applications) are made based on impact factors. Cambridge University Press is the only option that might lead to ISI indexing. Currently articles in the proceedings count as citations to the Journal of Cryptology, but they are not themself indexed. ISI indexing would be wonderful, but there will be a gap (also in citations being counted) of unforeseen length.

McCurley acknowledges the vast amount Preneel has done so far and the Board thanks him. McCurley also suggests that we might need a separate Board member to manage the editors of the Proceedings. It is agreed that Springer is the lowest risk and that Cambridge University Press is the highest risk option, but potentially with the highest reward.

Usenix gives us most control, which also means most responsibility for IACR. Berson suggests we need to have concrete proposals from all three before a final vote is made.

Preneel will present the current possibilities and insights at the membership meeting.

> Action Point **9: Preneel** *(Mid May)*:
> Schedule a phone conference in mid May to make a recommendation to the board.

11.5. **Publication bandwidth.** Vaudenay gives a brief presentation as a follow up to the (mostly e-mail) discussion started by Damgård. The record conference acceptance was in 2000 and only now acceptance numbers are getting close to it again (2011 was 1 paper fewer). Workshops are missing from this comparison (only TCC has been added since). Yet the number of submission has gone up by almost 60% from 1999 to now. Similarly, the number of members over the last years has gone up by a similar amount (partly due to CHES and TCC). Vaudenay's conclusion is that the number of accepted papers should go up by roughly 60% as well.

There is not enough time left to discuss possible solution in detail, but at the *Crypto'11* Board meeting a decision was already passed urgint the program chairs to increase the total number of acceptances. The decision is phrased as strongly as possible while still respecting the independence of program chairs.

> Action Point **10: Martijn Stam and Bart Preneel** *(no time set)*:
> Make the decision more widely known by telling PC, membership and integration in guidelines

12. Closing Matters

Preneel quickly recapitulates the main issues to discuss at the membership meeting.

> Action Point **11: Officers and Appointed Directors** *(no time set)*:
> Think about the tasks that come with the job.

After a brief review of action points, Preneel closes the meeting at 17.35.