MINUTES IACR BOARD MEETING *CRYPTO'11*

1. Opening

At 10.02 Preneel opens the meeting. People briefly introduce themselves. 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 a short break to celebrate Shrimpton's 40th birthday and an adjournment for lunch around noon.

1.1. **Roll of Attendees.** There are 20 attendees, holding a further 5 proxies.

Attendees (Elected). Josh Benaloh (Director –2011); Tom Berson (Director –2012); Christian Cachin (Vice-President –2013); Mitsuru Matsui (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). Matt Franklin (Journal Editor-in-Chief –2011); Shai Halevi (Membership Secretary –2011); Hyoung-Joong Kim (GC *Asiacrypt'11*); Xuejia Lai (GC *Asiacrypt'12*); Tom Shrimpton (GC *Crypto'11*); Nigel Smart (GC *Eurocrypt'12*); Yiqun Lisa Yin (GC *Crypto'12*).

Attendees (Representatives and Others). Tsutomu Matsumoto (Asiacrypt Steering Committee); Hilarie Orman (Archivist); Jean-Jacques Quisquater (CHES Steering Committee).

Absentees (Elected). Stuart Haber (Director –2011, proxy Benaloh); Antoine Joux (Director –2011, proxy Vaudenay); David Nacchache (Director –2012, proxy Pointcheval); Christof Paar (Director –2013, no proxy).

Absentees (Appointed). Helger Lipmaa (GC *Eurocrypt'11*); Christopher Wolf (Newsletter Editor –2012, proxy Stam).

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

1.2. **Minutes.** The minutes are approved without changes. The Board expresses its thanks to the secretary for the updated look of the minutes.

1.3. **SVN Repository.** Cachin introduces the new SVN repository. In principle all (non-sensitive) documents should be present on the repository, but for instance Program Chair reports might not be added. The idea is that it is used beyond just the meeting. Preneel thanks Cachin for his efforts.

1.4. **Action Points.** Preneel briefly reviews the status of action points identified from the Eurocrypt'11 meeting.

(1) (PC guidelines) postponed till Agenda Item 3.1.
(2) (Web reviewing for JoC) see Agenda Item 5.5
(3) (ethics guidelines) postponed till Agenda Item 3.1.
(4) (GC guidelines) this has been taken care of by Rose.
(5) (AC'13 clarification) the SC has checked and UAE has a strong will to organize AC'13; they will present a proposal later today (Agenda Item 10.1).
(6) (internal voting protocol) Benaloh has not updated Board voting guidelines yet, but he will update a new version on the svn server. Benaloh also has a document about Helios for the general IACR elections, which will be stored there.

> Action Point **1: Josh Benaloh** *(no time set)*:
> Update Board voting guidelines and provide Helios election guidelines.

(7) (IACR website overhaul) Cachin reports that Wolf has gone forward and made a start with some minor changes to the IACR website.

Date: UCSB, 14 August 2011.

> Action Point **2: Christian Cachin, Christopher Wolf, Shai Halevi, Kevin McCurley, Hilarie Orman** *(Eurocrypt'12 BoD)*:
> Present a concrete proposal regarding the future of the IACR website and the underlying database(s) and infrastructure driving it.

(8) (conference/workshop colocation) The Board approves Eurocrypt proposals sufficiently well in advance for the workshops to adapt if they feel that colocation is desirable. The relevant steering committees have discussed the general idea of colocation and their representatives give a brief summary. FSE is definitely interested, but for the near future the proposals do not match. The PKC position remains unchanged (namely they are positive). From TCC there is no answer yet. [They later indicated not to be interested in colocation.]

Quisquater mentions that CHES is considering colocation with Crypto again in 2013.

1.5. ***Crypto'11* Status.** The number of attendees is looking to grow beyond 400, which is very high for recent conferences. Shrimpton (GC *C'11*) thanks Qualcomm, Microsoft Research and Voltage for their funding, which allowed generous student support.

The biggest change is probably that all talks will be recorded this year and be put up on YouTube. Disadvantages might be that standard YouTube videos are at most 10 minutes (which could result in talks having to be cut up in multiple fragments) and that YouTube is blocked in certain countries. There have been experiments with videos at conferences before and the IACR server is capable of (archived) streaming. However, for a permanent solution it might need a dedicated volunteer (George Lipholdt is mentioned as potential candidate) or outsourcing.

Rogaway has prepared a short document (available on the svn) on the philosophy and the process behind his decision to provide this service, including a copy of the email to authors to obtain the relevant publication rights (based on Google's policy). Preneel thanks Rogaway and Shrimpton for their efforts.

Orman mentions that for travel of US students, the NSF is very generous and possibly students can look for stipends here as well. This would save IACR budget for other purposes.

Benaloh mentions that he experienced a glitch in the harvesting of email addresses for registering for the housing.

2. Officer's Report for Approval

2.1. **Treasurer's Report.** The situation is still looking healthy. Rose has, together with Handschuh, tried to close down the European accounts, but this is harder than it sounds. Some diversification is still needed. There are no objections from the Board that the IACR Treasury has a credit card available.

> Action Point **3: Greg Rose** *(before Eurocrypt)*:
> Send out a proposal for diversification of the IACR reserves.

Orman asks what the policy is on the (size of the) reserve. Preneel answers that in the past it has been decided at least one year should be available. In general the reserve is fairly stable, yet still slowly increasing. Preneel does not see an overall problem and reckons that in the future opportunities will arise to feed back money into the community, for instance by supplying more student stipends (and including the workshops in IACR's stipend program).

3. Guidelines for Approval

3.1. **Status of Revisions.** Cachin mentions that there are several documents dealing with the Ethics guideline. There is a policy on irregular submissions, there are guidelines for reviewers and there is an overarching ethics policy. These documents should be regarded as a whole (and have been edited as such). He mentions that other organization have more detailed guidelines and that the responsibility of the ethics committee is the handling of disputes.

Preneel brings up whether it should be allowed to submit in parallel to a conference and a journal. There have been changes in the policy in the past (based on how the program chair sets the call for paper). Halevi wonders whether this should be formally arranged and a discussion ensues, where the ACM policy (available from `www.acm.org/publications/policies/sim_submissions/`) is mentioned as an example. Eventually, the Board decides that, following roughly the ACM version:

Decision 1. *Simultaneous submission to journals and conferences without obtaining explicit authorization from both the Editor-in-Chief and Program Chair(s) will be prohibited.*

> Action Point **4: Christian Cachin** *(no time set)*:
> Incorporate the new double submission policy in the relevant guidelines.

Action Point **5: Shai Halevi** *(no time set)*:
Integrate a link to the relevant guidelines in the review website.

4. Appointees Reports for Information

4.1. **Newsletter.** Preneel briefly gives an update of Wolf's report. The recent innovations (twitter etc.) are clearly a step in the right direction.

4.2. **JoC Editor-in-Chief.** Franklin reports all is going well. The special issue with an open call for papers and editors from outside the usual board was a success and he wants to repeat the experiment.

4.3. **Membership Secretary.** Halevi reports that the membership has levelled. One issue is IACR's compliance with credit card regulations, which is needed to process with conference and workshop registration. Halevi also mentions his intentions to stand down and is looking for a successor (see also Agenda Item 6.1).

4.4. **Archivist.** Since last year the indexing of the archive has changed to CryptoDB. This has revealed several errors in the CryptoDB that are hard to fix for Orman (due to access control). Similarly, Orman would like to add links in the database to the copyright form, which is currently not the case.

Action Point **6: Christian Cachin, Shai Halevi, Hilarie Orman** *(no time set)*:
Rethink how copyright forms are checked and later archived.

Preneel thanks Orman for all the effort and the clear picture that she has provided.

5. Internal Committee Reports for Information

5.1. **Fellows Committee.** There are no new developments; the Fellows for 2011 will receive their plaque later during Crypto'11.

5.2. **Electronic Publishing Committee.** Progress has been made, but it is still too recent to discuss during the present board meeting. See also Agenda Item **??**

5.3. **Ethics Committee.** No further issues (see Agenda Item 3.1).

5.4. **Election Committee.** Vaudenay reports that the committee is a bit late with its nomination procedure, but it will post the nomination form online and distribute paper copies during Crypto.

Benaloh mentions that the Helios system has been updated to deal with approval voting. Preneel brings up that approval voting is currently only decided for Directors, not for Officers, and wonders whether we should change it for Officers as well (even though it only makes a difference if there are more than three candidates).

Decision 2. *The IACR Election for Officers will henceforth be conducted using full approval voting.*

5.5. **JoC web system evaluation.** Smart has tried several on-the-shelf open source packages. They all seem to require a slight change in the workflow from what is currently going on, but perhaps it is a change for the better. Minor changes to the software we could make ourselves, but major changes would be harder.

Action Point **7: Nigel Smart** *(no time set)*:
Discuss the findings related to potential JoC web systems in more detail with Franklin.

6. Appointments

6.1. **Membership Secretary.** Halevi will not be available for a further term, but he has been hunting down a successor. He is still in discussion with a couple of candidates and will report back to the Board, so they can decide before the end of the year. [abhi shelat was later appointed, see decision 12.]

Action Point **8: Shai Halevi** *(October 2011 [since completed])*:
Find possible successor(s) for Membership Secretary and report back to the Board.

6.2. **JoC Editor in Chief.** Preneel thinks Franklin is doing a good job and proposes to reappoint him. This is unanimously supported and Franklin accepts.

Decision 3. *Matt Franklin is appointed JoC Editor in Chief for the period 2012–2014.*

It is noted that the transition period between Maurer and Franklin was rather long, indicating that the Board should soon start to think already about the next Editor in Chief. Possibly a rolling system would be an option here as well. Preneel will take this up with Franklin.

7. Conferences since last BoD Meeting

7.1. ***Eurocrypt'11.*** It was an excellent conference and the Board thanks Lipmaa (GC *EC'11*) for his efforts.

8. Forthcoming Conferences for Information

8.1. ***Asiacrypt'11.*** The hotel room rate has been fixed (in Korean currency) and Kim (GC *AC'11*) reports that everything is looking well. The program will be announced shortly (42 papers have been accepted).

8.2. ***Eurocrypt'12.*** More sponsoring is coming in. Smart's (GC *EC'12*) main worry is the current volatility in USD–GBP exchange ranges. The accommodation poll showed 50–50 support for the college's dormitories.

8.3. ***Crypto'12.*** Yin (GC *C'12*) reports all is going well.

8.4. ***Asiacrypt'12.*** Due to recent inflation in China, costs have increased by 10 percent.

9. Steering Committee Reports and Workshop Proposals

9.1. **Asiacrypt.** (This point was treated chronologically after Agenda Item 10.1.) Matsumoto (Asiacrypt SC) will make sure that the SC will push for an alternative proposal for *Asiacrypt'13* as soon as possible.

9.2. **TCC.** There are no updates.

9.3. **PKC.** The SC has decided to put forward a modified proposal for *PKC'12* and the Board has already approved this by email.

9.4. **FSE.** The Board has already approved by email a proposal by the SC to hold *FSE'12* collocated with NIST's SHA-3 proceedings.

9.5. **CHES.** *CHES'10* went well.

Although *CHES'11* was moved to Nara, at the moment there are 150 people registered, so *CHES'11* looks on schedule to a healthy number of participants. An impressive amount of sponsoring has been acquired, some of it might be used to buffer against recent fluctuations in the exchange rate.

Quisquater (CHES SC) gives a presentation for a *CHES'12* proposal. Cachin thanks Quisquater and the Board unanimously approves the proposal.

Decision 4. *The Board approves the CHES'12 proposal, meaning that CHES'12 will be held in Leuven (Belgium) with Lejla Batina and Ingrid Verbauwhede as General co-Chairs and Emmanuel Prouff and Patrick Schaumont as Program co-Chairs.*

10. Conference Proposals for Discussion/Selection

10.1. ***Asiacrypt 2013.*** Thomas Martin temporarily joins the meeting. Martin presents the UAE bid for Asiacrypt 2013. Kim (past *AC* SC Chair) pledges his support. A discussion ensues focussing on the hospitality of the UAE to women and Israeli. Yin mentions that she went to the UAE and was welcomed, however she does recall a hefty visa deposit. Martin acknowledges that he cannot predict the visa application process.

The Board deliberates hard and long. The conclusion is that it is a very strong proposal, but the Board is uncomfortable with access for all nationals and does not approve the proposal. It is suggested that the UAE organize a smaller workshop first before resubmitting the proposal later.

10.2. **Program Chairs Reports.** Benaloh reports no special issues were mentioned in the PC reports.

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

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

Decision 5. *Phong Nguyen is appointed Program Chair (rolling co-chair) for Eurocrypt'13 and Eurocrypt'14. [Phong Nguyen subsequently accepted.]*

10.5. **Asiacrypt'12–'13.** There is a brief discussion to what extent the uncertainty about the location of *Asiacrypt'13* should or should not influence this appointment. It is noted that with the rolling co-chair the link between chair and conference has changed slightly. For background information, Xiaoyun Wang has already been appointed co-chair for Asiacrypt'12 and it would be best to appoint the other co-chair as soon as possible. Several excellent candidates are nominated, and after discussion a candidate is selected.

Decision 6. *Kazue Sako is appointed Program Chair (rolling co-chair) for Asiacrypt'12 and Asiacrypt'13. [Kazue Sako subsequently accepted.]*

10.6. **Crypto General Chair.** Several excellent candidates are nominated, and after discussion a candidate is selected.

Decision 7. *Helena Handschuh is appointed General Chair for Crypto'13. [Helena Handschuh subsequently accepted.]*

10.7. **Eurocrypt 2013 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 8. *Eli Biham is invited to deliver the Distinguished Lecture at Eurocrypt'13. [Eli Biham subsequently accepted.]*

11. STRATEGY

11.1. **IACR Publication: Strategy and Contract.** Preneel gives a brief presentation. There are several new challenges and opportunities, leading to three more or less orthogonal questions.

Currently attendees to a conference customariliy receive a printed copy of the proceedings, and members of the IACR receive printed copies of the Journal of Cryptology. The first question is whether the default should switch to a situation where participants resp. members will have electronic access by default, but will only receive a printed copy as a (payed) opt in. There have been some successful experiments with this before and the Board decides in favour.

Decision 9. *The IACR will move to a system with opt-in printed versions of the Journal of Cryptology for its members and of proceedings for its conference (and workshop) participants. The membership contribution will be changed (in due time) to reflect the opt in.*

A second question is whether we want to move to open access, where even non-members have fast and free access to papers published by the IACR. While open access can be an issue for both the Journal of Cryptology and the proceedings, the discussion concentrates on the latter (the IACR currently has two separate contracts with Springer: one concerning the Journal and a soon-to-expire one concerning the proceedings).

There is a discussion about the pros and cons of open access leading to a consensus that open access is the future. The main concern is how to implement it in a way that is neither too risky nor too costly. The Springer alternative providing the level of open access envisioned is quite expensive. The difference in price between access for members and attendees only versus fully open access is considerable and there is some discussion about different models on how to cover these higher costs. Alternatives to Springer are also mentioned, for instance, Usenix would be a cheaper alternative (but without some of the guarantees that Springer can offer us).

It is remarked that the IACR currently holds the copyright to its publications. If changes are made, it is important to keep track of copyrights.

Decision 10. *The IACR will move to open access for workshop and conference proceedings and find the best publisher to support this.*

The third and final question ties in with an email discussion started by Damgård. The claim is that the number of good papers submitted to our conferences is currently substantially higher than the number of accepted papers. (The workshops are excluded from this discussion, as this aspect falls under the remit of the respective steering committees.)

A possible solution would be to increase the number of accepted papers of the conferences. For Crypto and Asiacrypt this year the number is already just over 40; for Eurocrypt it was still considerably lower. A further increase would cause some practical problems, such as the physical size of the proceedings and the scheduling of the talks.

With the intended move away from paper-by-default, the first problem is not considered very severe. Scheduling talks is more challenging and several potential solutions are discussed, including having parallel sessions. For upcoming conferences parallel sessions are probably not an option (due to lacking infrastructure), but for future Asiacrypt and Eurocrypt proposals the potential to go parallel can be incorporated into the bids. For Crypto, the situation at UCSB is less clear.

Overall the majority of the Board feels an increase in bandwidth for the conferences and a corresponding guideline to the program chairs justified. The Board stresses that the precise number of accepted papers will vary depending on the number and quality of the submissions and the guideline does not take away the independence of Program Chairs (and their committees) to reject the papers they feel ought to be rejected.

Decision 11. *Conference Program Chairs (for Eurocrypt, Crypto and Asiacrypt) are expected to accept substantially more papers than used to be the case and to work with their General Chair for the logistics to make this possible (using extra slots, shorter talks and parallel session).*

As an alternative model to consider sometime in the future perhaps, VLDB is briefly mentioned.

11.2. **ICT Infrastructure.** The ICT Infrastructure is somewhat fragmented. It is suggested that if IACR were to partner with Usenix, they might be able to provide part of the solution (as such a change would likely require a further rethink on IACR's end). Action will be undertaken (e.g. Action Point 2 and ongoing negotiations by the President with Springer and possibly alternative publishers).

11.3. **IACR Membership Rules.** Halevi brings up a problem with the current system, where attending an IACR conference or workshop in year x includes membership for year $x+1$, but not x. This can lead to surprises among people attending one of the earlier workshop, yet finding they are not eligible to vote later in the year.

Prior to the meeting, several alternative systems were discussed by email, but none seemed without problems. It is noted that the current system for individual members (not tied to conference attendence) already makes it possible to become a member for the current year (by paying the relevant membership fee).

11.4. **Electronic voting update.** Benaloh mentions that the backend has changed, but he does not believe extra testing is necessary.

11.5. **Future scheduling of workshops.** This point has already been covered by other discussions.

11.6. **Review of bylaws.** Stam briefly mentions that he noticed some small discrepancies between practice and what is in the Bylaws.

12. Closing Matters

Cachin thinks that adding an additional phone meeting might be beneficial. One option would be to have a meeting at Asiacrypt with board members not attending dialling in.

Vaudenay brings up some recent problems with a conference that had the ICW stamp. Preneel agrees with this particular case, but does not feel like there is currently a big problem.

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

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

13. Intermediate Board Decisions

Decision 12 (3 November 2011)**.** *The Board appoints abhi shelat as membership secretary for the period 2012–2014. [abhi shelat subsequently accepted.]*

Decision 13 (26 February 2012)**.** *The Board approves the PKC'13 proposal, meaning that PKC 2013 will be held in Nara (Japan) with Goicihiro Hanaoka as General Chair and Kaoru Kurosawa as Program Chair.*

Decision 14 (26 February 2012)**.** *The Board approves the TCC'13 proposal, meaning that TCC 2013 will be held in Tokyo (Japan) with Masayuki Abe and Tatsuaki Okamoto as General co-Chairs and Amit Sahai as Program Chair.*

Decision 15 (26 February 2012, 17 March 2012)**.** *The Board approves the FSE'13 proposal, meaning that FSE 2013 will be held in Singapore (Singapore) with Jian Guo and Thomas Peyrin as General co-Chairs and Shiho Moriai as Program Chair.*