MINUTES IACR BOARD MEETING *CRYPTO'12*

UCSB, 19 AUGUST 2012

1. Opening Matters

At 10.06 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 21 attendees, holding a further 4 proxies.

Attendees (Elected). Josh Benaloh (Director –2014); Tom Berson (Director –2012); Christian Cachin (Vice-President –2013); Shai Halevi (Director –2014); Mitsuru 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); Nigel Smart (Director –14, GC *Eurocrypt'12*); Martijn Stam (Secretary –2013); Serge Vaudenay (Director –2012).

Attendees (Appointed). Matt Franklin (Journal Editor-in-Chief –2014); Helena Handschuh (GC *Crypto'13*); Xuejia Lai (GC *Asiacrypt'12*); Satya Lokam (GC *Asiacrypt'13*); Yiqun Lisa Yin (GC *Crypto'12*).

Attendees (Representatives and Others). Ivan Damgård (TCC Steering Committee); Tsutomu Matsumoto (Asiacrypt Steering Committee); Kevin McCurley (Database Administrator); Hilarie Orman (Archivist).

Absentees (Elected). David Nacchache (Director –2012, proxy Pointcheval);

Absentees (Appointed). Aggelos Kiayias (GC *Eurocrypt'13*, proxy Preneel); abhi shelat (Membership Secretary –2014); Christopher Wolf (Newsletter Editor –2014, proxy Paar).

Absentees (Representatives and Others). Jean-Jacques Quisquater (CHES Steering Committee, proxy Paar).

1.2. **Minutes.** The minutes of both the BoD and membership meetings at *Eurocrypt'12* are approved with some minor changes.

Stam calls for a volunteer to make minutes of the *Asiacrypt'12* membership meeting, as he anticipates he will unfortunately not be attending.

1.3. **Action Points.** Preneel briefly reviews the status of action items identified from the *Eurocrypt'12* meeting.

(1) (Election documentation) Preneel notices this has been done and it will be discussed later.
(2) (Web volunteers) Preneel reports he has found three people with IT experience. Those responsible from IACR's perspective can contact these volunteers.
(3) (Guidelines incorporation) Halevi has done this.
(4) (JoC web-interface) Smart and Franklin report that there has been no concrete progress. The action item is maintained with a deadline added.

> Action Point **1: Smart, Franklin, McCurley** *(End of April 2013)*:
> Try to find a working solution for a web-interface for the JoC reviewing process.

(5) (Reserve diversification) Rose says that little progress has been made due to turmoil at the bank. It is no longer clear a signed board resolution is needed, so the point is dropped.
(6) (Audit committee) Berson has done this, see Agenda Item 2.1.
(7) (Committee survey) Stam reports no progress has been made. The action item is maintained with a deadline added.

> Action Point **2: Martijn Stam** *(1 October 2013)*:
> Keep better track of all the various committees.

(8) (Conference template) Rose reports no progress has been made. The action item is maintained with a deadline added.

Action Point **3: Greg Rose** *(1 November 2013)*:
Sort out the template to deal better with student stipends and free attendees.

(9) (Publishing progress) Preneel says there is a recommendation about publishing, to be discussed later, see Agenda Item 10.1.

(10) (Bandwidth dissemination) Preneel mentioned he has told the relevant programme chairs and he has announced the decision at the *Eurocrypt'12* membership meeting.

Action Point **4: Stam** *(1 October 2012)*:
Add the bandwidth expectations to the PC guidelines.

Action Point **5: Josh Benaloh** *(1 October 2012)*:
Make a 1 page update on recent IACR policy changes for program chairs.

(11) (Job descriptions) No one comes forward with news. Preneel offers to take the lead on this topic.

Action Point **6: Preneel** *(1 January 2013)*:
Think about the tasks that the officers and appointed directors have to perform.

1.4. ***Crypto'12* Status.** Yin reports there are already 340 attendees, of which more than 25% students. There are five sponsors resulting in a record amount of sponsoring. Yin has achieved 10.000 USD for NSF funding for student stipends and she thanks Orman for pointing out this possibility. She expects this funding will be available for future Crypto conferences as well. She is also happy with the large percentage of female recipients of stidents.

The proceedings are one page below the limit of a single LNCS volume. Since the page limit was reduced to 16 pages, authors were given the opportunity to publish a link to a full version on the program. This year is also the first time that the paper proceedings are opt-in. Roughly 15% of the participants opted in through online registration. All participants will receive a USB stick with an electronic copy of the proceedings. There is a brief discussion about the best way to present and produce the electronic proceedings, for instance using multiple files or a single, hyperlinked PDF.

Yin mentions that parallel sessions were discussed, but in the end it was not yet needed. There will be video recordings, concentrating on the slides (as for *Eurocrypt'12*) rather than on the presenters (*Crypto'11*). Cachin calls for a person to take responsibility for a consistent policy. McCurley has done this so far and mentions the possibility of live broadcasting. Benaloh asks whether the traffic to existing videos indicate whether the effort creating the videos is worthwhile.

Action Point **7: McCurley and Cachin** *(no time set)*:
Find somebody responsible for overseeing consistency of the recording and archiving of videos of presentations at IACR events.

Preneel thanks Yin for doing an excellent job.

2. Officer's Report for Approval

2.1. **Treasurer's Report.** Rose notices that his alarm at *Eurocrypt'12* was due to a double counting mistake, so we are quite safe so far and an audit committee is not strictly needed.

Berson has created a draft proposal for the running of an audit committee and he provides some background details. Following a brief discussion, various minor changes are mentioned. It is suggested to have audits whenever there is a change of treasurer, or once every three years (coinciding with a treasurer's term). For this reason, the audit committee members will be appointed for a period of three instead of two years. It should be noted that it will remain to the discretion of the audit committee to decide when (and how often) to audit.

To make the pool of possible people with sufficient expertise higher, only one audit committee member needs to be a board member (not necessarily elected) and the restriction on serving at most twice is relaxed to serving at most two consecutive terms.

Decision 1. *With some minor changes, the audit committee document is approved.*

Decision 2. *Tom Berson, Christof Paar, Helena Handschuh are appointed to the audit committee for a period of three years.*

Action Point **8: Cachin and Stam** *(1 October 2012)*:
Archive the audit committee document and the board voting guidelines.

Rose continues his discussion of the current financial state of the IACR. The financial results over the last couple of years are negligble. His attempts to diversify the reserves have been frustrated by a reorganization of the financial instution he was in discussion with, resulting in the people he was talking to no longer being available. Consequently, he has not pursued the issue any more.

McCurley inquires whether the IACR can hire people and if so, under which restrictions. It is not possible to hire (or financially reward in any manner) the directors, but hiring family of directors is probably allowed. Hiring people would also necessitate auditing.

3. Guidelines for Approval

3.1. **Board Voting Guidelines.** Benaloh did an excellent job. There is a small issue regarding the role of the President. It is suggested that if the President is not present, the presiding officer will only use its vote to break a tie.

3.2. **Evoting Guidelines.** Benaloh is on the committee this year and expects to update the guidelines after the election for next year.

> Action Point **9: Josh Benaloh** *(1 January 2013)*:
> Update the evoting guidelines.

3.3. **General chair guidelines.** Not of relevance.

3.4. **Discussion of other revisions needed.** Cachin is not aware of a further need for changes. He does requests all guidelines to be typeset in LaTeX.

4. Appointees Reports for Information

4.1. **Newsletter.** Preneel (obo Wolf) thinks Wolf is doing an excellent job. The increase of live updates on the website minimizes the need of a newsletter. General chairs are encouraged to use channels (as part of the website's newsfeed) to interact with the membership. Rose notices that there are still a few types of news items that do not fit in any of the currently defined categories (e.g. people looking for jobs, general discussions).

4.2. **JoC Editor in Chief.** Franklin reports that the publication pipeline is steady. The impact factor has gone down significantly, but it is not clear why this is the case. Preneel remarks he will soon shift his attention to the journal and will ask Springer for a possible explanation.

4.3. **Membership Secretary.** Preneel (obo shelat) mentions that there has been a slight increase in the membership numbers with a steady number of students. Preneel thanks shelat for his excellent work.

4.4. **Archivist.** Orman says that the archive is on track. She also mentions that contact with programme chairs can still be hard. She reminds the board that the archive project was started to make the papers freely available online and expresses the hope IACR will move to open access. The Board thanks Orman for her excellent work.

4.5. **Database.** McCurley has compiled a list of open problems, for instance a forum and support for videos are challenging. Overall there has been a tremendous amount of progress this year. Preneel thanks McCurley, Cachin, Wolf, and Smart for all the progress that has been made.

5. Internal Committee Reports for Information

5.1. **Electronic Publishing Committee.** Postponed to Agenda Item 10.1

5.2. **Ethics Committee.** According to Cachin, no problems have come to the direct attention of the committee. There are however a few problems on the horizon, both at *Crypto'12* and *Asiacrypt'12* an ethics-related issue was informally reported.

Several concrete actions to raise awareness of ethical issues among our membership (and beyond) are discussed. Vaudenay suggests an audit committee for ethical issues. A discussion ensues whether there is an ethics problem within our community and how to deal with it (for instance, with potential conflicts of interests for subreviewers). The feeling is that in general the current system works, but there are still failures. Increasing the visibility of the IACR's ethics guidelines is desired.

> Action Point **10: Ethics Committee** *(no time set)*:
> Increase awareness of ethics by writing a news item on the official announcement channel.

5.3. **Election Committee.** Benaloh reports that he has been elected as chair; Pointcheval will be the returning officer. Apart from that, there has been little progress.

He also reports on a technical problem that appears in Helios and other protocols related to the use of Fiat–Shamir proofs. As a result, if the administrators colluded, they could have breached the security of the election. There is no reason to believe the 2011 elections were compromised, the problem will be fixed in time for the 2012 elections.

5.4. **JoC web system evaluation.** Nothing to say.

6. Conferences since last BoD Meeting

6.1. ***Eurocrypt'12.*** Smart (GC *EC'12*) reports that the conference went well and a surplus is expected. The Springer invoice is still pending.

7. Forthcoming Conferences for Information

7.1. ***Asiacrypt'12.*** Lai (GC *AC'12*) reports on the progress. Just over 40 papers have been selected. It is not yet clear whether there will be a free afternoon or not. The registration fee will be fixed soon. Preneel reminds Lai of an existing IACR decision that makes available funding for local students.

7.2. ***Eurocrypt'13.*** Preneel gives an update obo Kiayias (GC *EC'13*).

7.3. ***Crypto'13.*** Handschuh (GC *C'13*) reports that preparations are on track and a venue has been selected. Discussions with Sally (UCSB) are scheduled for this week and discussions regarding *CHES'13* colocation for later.

7.4. ***Asiacrypt'13.*** Lokam (GC *AC'13*) provides some backgrount on a second venue under consideration. It is closer to the city, in a relatively quiet area, with some other hotels around. It might not be suitable for parallel sessions and lunches would be outside.

8. Steering Committee Reports and Workshop Proposals

8.1. **Asiacrypt Steering Committee.** Matsumoto reports that *Asiacrypt'15* proposals will be discussed at *Asiacrypt'12* in Beijing. His own term on the steering committee will come to an end and next year there will be another representative from the steering committee.

8.2. ***TCC'13* Status.** Damgård (SC *TCC*) reports that everything is on track. Negotiations for *TCC'14* are ongoing.

8.3. ***FSE'13* Status.** Preneel (SC *FSE*) reports that everything is on track.

8.4. ***PKC'13* Status.** Pointcheval (SC *PKC*) reports all is going ok. There is a proposal in early stages to host *PKC'14* in Buenos Aires.

8.5. ***CHES'12* status and *CHES'13* budget.** Paar (obo SC *CHES*) reports that *CHES'12* will commence in a few weeks. New this year are tutorials at the beginning of the conference. There are currently 310 registrations with roughly 20% students. Roughly 30% of the participants opted in for the paper proceedings. The CHES program cochairs gave some feedback regarding the running of the program committee, especially in relation to the supporting IT.

There is still no budget for *CHES'13*.

> Action Point **11: Paar** *(1 October 2013)*:
> Get a budget for CHES'13.

9. Conference Chairs

9.1. **Program Chairs Reports.** Preneel remarks that there are two reports from *Eurocrypt'12*, a short one for the Newsletter and a longer one for the Board. There were further reports from *Crypto'12* and *CHES'12*, but several reports were missing and need to be chased.

9.2. **Program and General Chair List Maintenance.** Stam gives an overview of the changes made to the various lists. The board chimes in with further suggestions.

9.3. **Eurocrypt'14–'15.** Phong Nguyen has already been appointed as one of the co-chairs for *Eurocrypt'15*. Several excellent candidates are nominated, and after discussion a candidate is selected.

Decision 3. *Elisabeth Oswald is appointed Program Chair (rolling co-chair) for Eurocrypt'14 and Eurocrypt'15. [Oswald subsequently accepted.]*

9.4. ***Crypto'14* General Chair.** Several excellent candidates are nominated, and after discussion a candidate is selected.

Decision 4. *Alexandra Boldyreva is appointed General Chair for Crypto'14. [Boldyreva subsequently accepted.]*

9.5. **Crypto 2014 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 5. *Mihir Bellare is invited to deliver the Distinguished Lecture at Crypto'14. [Bellare subsequently accepted.]*

10. Strategy

10.1. **IACR Publication Strategy.** Preneel reports on the investigation by him, McCurley, Cachin, and Smart. They looked at three alternatives, namely open access with Springer, a renegotiated contract with Springer, and a new solution with Cambridge University Press.

After a deeper investigation, Cambridge University Press carries a risk to both the impact factor and access to back catalogue. Orman asks whether we have a metric to determine how many people are affected by ISI indexing. Preneel answers he does not know, but he has the impression the number is increasing. Several board members give their local view: Smart mentions that in Bristol the importance depends very much on the topic with EE being more affected than CS; a similar situation is reported from Japan (for EE indexing is serious, for CS and crypto less so); in China the indexing is important. There is a discussion whether we should try to survey the impact of ISI in more detail, but the outcome of such a survey will not change much.

Preneel continues to discuss the Springer contract, as he feels that Springer open access is too expensive. The consensus of the Electronics Publishing Committee (EPC) is that the current draft contract is too complex, but at the same time the impression is that it would mean everybody will get access to papers directly. Under the proposed contract, there will be (at least) three versions of a paper:

- The official LNCS version;
- The author version (technical term from the publisher), we could call it IACR version;
- The full version(s): Assuming 25% percent is novel.

There are technical problems with the version management, for instance when both the author version and the full version are on eprint. An additional problem is that many versions could lead to a dilution of citations. From an archiving perspective a fixed version is beneficial, from an authors perspective having a variable version can be desirable.

If we abandon USBs there will be a significant cost reduction. The EPC thinks to invest this money in support staff.

After extensive discussion, the final recommendation is put to the vote. With 17 in favour, 2 against, and 2 abstentions the following is accepted:

Decision 6. *The Board decides to go forward with the Springer contract and requests the President to finalize negotiations and sign the contract.*

Orman expresses her regret that so little progress towards true Open Access (where the author retains copyright) has been made.

The Board thanks the EPC for doing a good job under very difficult circumstances.

The next question is i) how to present the Board's decision process to the membership, making it as clear and easy as possible for people to understand the contract under discussion and ii) how to implement the new contract. Preneel suggests that the latter step will be substantial and will likely require a committee and possibly subcontracting.

Action Point **12: Publication Committee** *(1 December 2012)*:
Take care of the implementation of the new contract.

10.2. **Website redesign.** McCurley explains that the most important missing link at the moment is the capture of metadata of articles.

The authentication system can be improved to allow more fine-grained access control. Vaudenay remarks that an improved authentication system could also benefit the electronic voting (where currently Helios authentication is completely separate process) and Cachin suggests the possibility of an authenticated forum on the IACR server.

Preneel thinks it is important to have a discussion forum, as the membership meetings provide only very limited opportunity for discussion. There is a question whether non-members should be able to contribute as well. McCurley suggests to have a moderated forum. It is not clear how to get traction.

Decision 7. *The Board decides to experiment with a discussion forum.*

Action Point **13: McCurley** *(no time set)*:
Find a moderator and a technical solution for a possible IACR discussion forum.

Rose mentions that future conferences are not yet easily retrievable from the website. Overall, Handschuh thinks the new design looks really cool.

There is a discussion about third party JavaScripts on the IACR website (such as a Facebook “like” button or Google maps). The board is concerned about the risks involved and asks the webmaster to use diligence when third party Java-scripts are added.

Decision 8. *The Board approves the publishing of Canetti’s opinion in the newsletter.*

10.3. **IACR Archiving Scope.** Preneel explains that there has been a question about the use of old photos taken at past IACR conferences. Berson provides historical background that the photos were taken without asking for permission from the people on the page (the assumption was that the paranoid people would stay away from the view).

Action Point **14: Orman and Stam** *(no time set)*:
Make a policy on what we want to archive and how, including dealing with permissions

10.4. **Program balance at IACR flagship conferences.** There have been several opinions made available concerning the program balance at IACR flagship conferences. Smart agrees with the note by Standaert, who gives a (subjective) partitioning of the flagship conferences in the subdomains roughly covered by the workshops and concludes that especially the CHES community is underrepresented.

There seems to be consensus about the possibility to classify papers along the communities. For the accepted papers there appears an imbalance: part of the cryptologic community is structurally underrepresented. The question is how to bring balance to the fore. Preneel believes it is a cultural chicken and egg problem. He also remarks that the program chair guidelines already stipulate that during selection of the program committee a few places should be left open to improve balance (in discussion with the PC contact).

A few options to improve balance further are debated, including the effects on program chair and committee independence. Suggestions mentioned are program chair selection and imposing quota on the program or program committee composition (to better represent the various communities).

Decision 9. *The Board decides that the balance ought to be improved and encourages program chairs to be aware of program balance and take action accordingly.*

11. Closing Matters

There seems to be more and more fraud happening regarding papers being plagiarized in other journals. Orman suggests active action from the IACR to prevent against criminal enterprise. The first problem is to detect the offending cases (often hidden behind a paywall). A second problem is that the potential for follow up is unclear. Paar notices that the damage for the IACR and its membership so far is limited: as long as the plagiarized paper is hard to obtain, it will not be cited.

Action Point **15: Orman** *(no time set)*:
Investigate and/or create a tool to detect plagiarism of IACR copyrighted material.

11.1. **Draft agenda for general meeting of members.** Preneel quickly recapitulates the main issues to discuss at the membership meeting.

11.2. **Review of Action Items.** After a brief review of action points, Preneel closes the meeting at 17.35.

12. Intermediate Board Decisions

Decision 10 (14 January 2013)**.** *The CHES 2013 budget is approved.*

Decision 11 (14 January 2013)**.** *The Board approves the TCC'14 proposal, meaning that TCC 2014 will be held in UCSD, California (USA), on Feb 24-26 (2014) with Mihir Bellare and Daniele Micciancio as General co-Chairs Yehuda Lindell as Program Chair.*

Decision 12 (31 January 2013)**.** *The Board approves the PKC'14 proposal, meaning that PKC 2014 will be held in Buenos Aires (Argentina) with Ariel Waissbein as General Chair, Juan Garay as General co-Chair, and Hugo Krawczyk as Program Chair.*

Decision 13 (31 January 2013)**.** *The Board approves a budget of 3000 USD for student support on improving the IACR webreview software.*