MINUTES IACR BOARD MEETING *EUROCRYPT'14*

COPENHAGEN, 11 MAY 2014

1. Opening Matters

At 9.38 Cachin opens the meeting and he briefly goes around for an introductory round, confirming attendees and establishing 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 16 attendees, holding a further 5 proxies.

Attendees (Elected). Michel Abdalla (Director –2015); Josh Benaloh (Director –2014); Christian Cachin (President –2016) Anna Lysyanskaya (Director –2015); Bart Preneel (Director –2016, FSE Steering Committee); Greg Rose (Treasurer –2016); Nigel Smart (Vice-President –2016); Martijn Stam (Secretary –2016); Moti Yung (Director –2014).

Attendees (Appointed). Alexandra Boldyreva (GC *Crypto'14*); Gregor Leander (GC *Eurocrypt'14*); Svetla Petkova-Nikova (GC *Eurocrypt'15*); Thomas Ristenpart (GC *Crypto'15*); abhi shelat (Membership Secretary –2014).

Attendees (Representatives and Others). San Ling (Asiacrypt Steering Committee); Jean-Jacques Quisquater (CHES Steering Committee).

Absentees (Elected). Tom Berson (Director –2015, proxy Benaloh); Shai Halevi (Director –2014, TCC Steering Committee, proxy Lysyanskaya); Christof Paar (Director –2016, proxy Leander); David Pointcheval (Director –2013, PKC Steering Committee, proxy Abdalla).

Absentees (Appointed). Ivan Damgård (Journal Editor-in-Chief –2016); Steven Galbraith (GC *Asiacrypt'15*; Matt Franklin (Journal Editor-in-Chief –2014); D.J. Guan (GC *Asiacrypt'14*, proxy Ling); Christopher Wolf (Communications Secretary –2014).

Absentees (Representatives and Others). Kevin McCurley (Database Administrator); Hilarie Orman (Archivist).

1.2. **Minutes.** The minutes of both the BoD and membership meetings at *Crypto'13* are approved with some minor changes.

1.3. **Action Points.** Cachin briefly reviews the status of action items identified from the *Crypto'13* meeting.

- C13-2 Cachin updated the budget template on the svn but still needs to discuss more. This will be done by the end of the week. Preneel notices that rolling out is not trivial (FSE'15).
- C13-3 + C13-4 Benaloh has notes on things, but does not have the actual advice. Smart asks how active are we in advising conference program chairs to the chair contact.

Action Point **1: Smart, Benaloh** *(no time set)*: Better PC contact process desired, update guidelines.

- C13-5 Preneel has not done this yet, but thinks that with a change of the guard, perhaps Cachin should take the lead.

Action Point **2: Preneel, Cachin** *(no time set)*: Discuss officers and appointees tasks

- C13-6 Still dormant, taken of the list as action point. Benaloh remarks we can concentrate on supporting this for GC first, rather than mandating. It would require early contact with chairs etc. Leander suggests to add to the budget. Cachin calls for volunteers.
- C13-8 Been done once
- C13-9 Orman has made an initial draft, to be discussed later. There are cultural differences and an increasing amount of pictures. The best way would be to add something to the registration form.

- C13-10 Authentication came up to make available for instance an IACR svn server.
- C13-11 Preneel has not heard from his Springer contact, despite prompting. He reckons that there is still a paper-copy obligation. Rose notices that the costs for the journal has gone up considerably. The costs should go down with the opt-in mechanism, but for *Eurocrypt'14* the registration system was not yet up-to-date.

> Action Point **3: Preneel, Cachin** *(no time set)*:
> Sort out a new JoC Springer contract

> Action Point **4: Preneel, Cachin, shelat** *(no time set)*:
> Implement the JoC opt-in system on the registration and with UCSB/Springer

- C13-12 Officialize Lars's page on the IACR, adding registration fees and attendance. Additionally there has been an e-mail discussion related to keeping track of gender.
- C13-13 Preneel has not spoken with Springer, this can be subsumed by publication pipeline optimization.
- C13-16 Not clear whether the website has been updated or not.
- C13-17 Letter has been written, but no answer so far.
- T04-6 Online access to proceedings: has been simplified.

> Action Point **5: Smart** *(no time set)*:
> Is taking the lead on updating the website, specifically access to publications.

> Action Point **6: Preneel** *(no time set)*:
> Speak to lawyer re who can legally vote

1.4. ***Eurocrypt'14* Status.** Leander (GC *EC'14*) reports that a significant number of students had their registrations waived. Only if multiple students from the same university applied he checked more rigourously whether the requests were reasonable. Currently registration stands at 321 and the budget seems fine.

There is a discussion related to the complexities of differences in VAT regulations from country to country.

Cachin thanks Leander for organizing.

2. Officer and Appointee Reports

2.1. **Treasurer's Report.** Rose has sent out a report and gives some background information. There was a slight delay partly due to software hiccoughs.

There is a discussion related to the desirability of a European bank account. IACR used to have two, but these accounts have been terminated as a result of practical difficulties (both with the banks, but also due to US reporting regulations).

Cachin thanks Rose for his hard work.

2.2. **JoC Editor in Chief.** Smart (obo Franklin and Damgård) reports that the two editors have agreed on a hand-over.

2.3. **Program chair reports.** It is requested for the program chair reports to be made available on the svn, provided they do not contain sensitive information.

2.4. **Communications Secretary.** As a result of the recent Bylaws change, the Newsletter editor has been relabelled Communications Secretary. Cachin (obo Wolf) reports that he will be vacating his job as Communications Secretary position over the summer.

Decision 1. *Wolf is appointed Communications Secretary from January 2014 to July 2014.*

Cachin thanks Wolf for his dedication over the years.

2.5. **Membership Secretary.** shelat remarks that overall membership is lower this year as last year, partly as a peak in the membership in 2013, and partly a result of lower attendance at *Asiacrypt* last year. Both can be attributed to geographical factors.

Cachin thanks shelat for his contribution.

2.6. **Archivist.** Cachin (obo Orman) highlights a number of points from Orman's report.

2.7. **Database Administrator.** Cachin (obo McCurley) clarifies that Halevi is also involved.

3. Internal Committee Reports

3.1. **Fellows Committee.** Cachin (obo McCurley) reports that the announcement of 2014 inductees has been delayed. Inducted will be Ran Canetti, Antoine Joux, Eyal Kushelevitz, and Moti Yung.

Cachin thanks the Fellows committee, but would like to encourage the Fellows committee to update their internal guidelines to ensure Fellows can opt to be inducted at Eurocrypt.

3.2. **Audit Committee.** There is no report from the audit committee, but Rose mentions that Andy Clark has volunteered to help with revising the processes and administration handled by the Treasurer.

3.3. **Ethics Committee.** Smart mentions several changes to internal procedures. In particular, when an incident is reported and based on its findings, the Ethics Commitee will keep a private list of grey area incidents. This list will be available to the Program Chair liaison (who is expected to sit on the Ethics committee).

Stam mentions that those accused of unethical behavior should have the opportunity to present their case, except for summary dismissals by the Ethics Committee. Preneel adds that people on the list should know whether they are on the list or not.

There is a small discussion of possible ethics infringements. Preneel points out that when external advice is sollicited, confidentiality needs to be maintained. It is noted that the Bylaws allow to scrap membership as a sanction, which should be taken into account in the ethics guidelines.

Ristenpart asks what approaches other professional organizations take.

Action Point **7: Smart** *(no time set)*:
Update the ethics guidelines to clarify the process of enhanced organizatorial memory

Cachin thanks the Ethics committee.

3.4. **Schools Committee.** A short description of the schools initiative is already on the website. Rose clarifies that IACR's financial support for schools comes from the general IACR budget, irrespective of a surplus. The final budget available for schools will be approved by the Board.

Abdalla reports they have already been contacted by some summer schools that will take place this July. Schools can already request ICW status, as there are no finances are involved.

Cachin thanks all those on this new committee.

3.5. **Publications Committee (ad hoc).** There is nothing to report.

3.6. **IT Committee (ad hoc).** There is nothing to report.

4. Appointments

4.1. **Ethics Committee.** By unanimous decision the Ethics committee for 2014 is constituted.

Decision 2. *Josh Benaloh (PC liaison), Tom Berson, and Nigel Smart (chair) are appointed to the Ethics Committee for the 2014 calendar year.*

4.2. **Election Committee.** Cachin notes that the terms for Benaloh, Halevi, and Yung (who took over Smart's Directorship) come to an end this year. The Board unanimously elects an Election Committee as follows.

Decision 3. *Michel Abdalla (returning officer), Anna Lysyanskaya, and Bart Preneel (chair) are appointed to the Election Committee for the 2014 election.*

5. Guidelines

5.1. **Bylaws, revised in 2013.** Stam reports that the updated Bylaws are available on the website.

5.2. **Updated ICW Guidelines.** Cachin reports that he has updated the guidelines for events that would like to be held 'in cooporation with' IACR. He has put the new guidelines on the website.

5.3. **Cryptology Schools guidelines.** These guidelines have been approved and are on the website.

5.4. **General chair guidelines.**

Decision 4. *The updated general chair guidelines are approved.*

5.5. **Program chair guidelines.** Not all changes resulting from the new publication process and recent Board decisions have been incorporated into the guidelines.

Decision 5. *The Board appoints Josh Benaloh and Nigel Smart to the PC guideline update committee*

Action Point **8: PC Revision Committee** *(no time set)*:
Update PC guidelines

5.6. **Collecting and publishing attendance statistics.** There has been an extensive email discussion regarding the keeping track of especially gender as part of conference registration. Lysyanskaya remarks that the main goal are the statistics. Smart believes this information will show whether the IACR is improving gender balance. Cachin clarifies that counting this data can be used for affirmative action.

Benaloh is supportive of increasing gender balance, however he does not agree to redress past discrimination with further discrimination. He personally finds the question offensive and, on principle would refuse to answer these questions. Stam concurs and remarks there might be a cultural component to how the question is perceived by people.

Preneel considers collecting the sums fine, but spots an implementation issue, for instance it may not be desirable to keep gender in the membership database. This leads to two decisions relating to the collection of gender statistics: one on the principle, and one on the implementation (voted for in the order presented below).

Decision 6 (11 in favour, 4 against, 5 abstentions.)**.** *The IACR should collect gender information for the purpose of statistics.*

Decision 7 (14 in favour, 4 against, 2 abstentions.)**.** *Total gender counts will be collected per event (with no further subdivisions) by an optional question but data is not recorded in a personally identifiable way.*

5.7. **Discussion of other needed revisions.** Cachin remarks there are no further revisions needed

6. Publications

6.1. **Implementation of current publication model.** Cachin proposes to hire someone as a communications administrator to perform the necessary checks and actions in support of the publication process as a routine matter. The person would have to maintain cryptoDB (once the IT side is sorted out by the IT committee) and should also be able to run LaTeX. Benaloh wants to make sure that we are contracting for services, not hiring a part-timer.

KU Leuven would be one possible service provider (it is task complementary to UCSB's membership services). Preneel mentions that he envisions the first year as a pilot to determine how much work will be involved long term. The Board in general is in favour. Cachin will return to the Board at *Crypto 2014* with a more detailed report and a concretely costed proposal.

Action Point **9: Cachin, Preneel** *(1 August)*:
A more detailed and concrete, costed proposal for contracting out publication process aid

There is a subsequent discussion regarding versions on eprint.

6.2. **eprint Update.** Smart notices that if people have a paper on eprint that is subsequently published elsewhere, the eprint version can no longer be updated as the authors will have to sign over copyright. Smart suggests to ask IEEE and similar organizations to put eprint on their list of accepted archives, etc.

Action Point **10: Smart** *(no time set)*:
Chase other organizations to allow possible copyrighted material on eprint.

7. Future publications model

7.1. **Strategy discussion.** Cachin and Smart recount the story so far. One of the key questions is whether the publication model that has served us well since 1981 will still be the best choice for 2021 (and beyond). The four aspects of the publications model identified are

(1) Open access: there are external forces towards increasing open access, the main questions are cost-related.
(2) Indexing: both the indexing process and the value attached to it are primarily externally driven.
(3) Latency and reviewing workload: the latency of journals in other fields beats our conferences. It directly affects the community and jointly we have a lot of control.
(4) Scientific integrity: the community has changed by increased rigour through proofs, but full versions are not always reviewed.

Yung wants to look organically at our community with less emphasis on external constraints. Active researchers themselves rely more on eprint for fresh results than on the formal publications. Nonetheless, he recognizes the importance of formal publications. He wonders whether it is possible to have conferences as successful as the current IACR ones, yet still have ISI indexing. He points out that stickyness of reviews for a journal (as a result of multi-round reviewing) is not absolute as one can still change journal.

Lysyanskaya does not like the strawman proposal and points out that we should not change our entire business model based on the hope of ISI indexing. She recalls her proposal to have special issues of the Journal of Cryptology. The difference with the current model is that you keep the original reviewers and there will be strict deadlines. For further discussion, refer to the *Crypto'13* BoD minutes. Yung suggests to maintain the same reviewers for a full journal version of a paper as for the conference submission, though Preneel doubts reviewers would favour such a set up.

There is a discussion about page limits and whether increasing page limits for proceedings would deliver value without incurring costs. Preneel believes that formally publishing unreviewed parts of a paper should be considered scientific fraud, so changing page limits does come at a price (increased reviewing load). Smart argues that the same limit should apply to submissions as to the publications. shelat believes that writing is enough even if it does not get reviewed and he would like to increase the page limit for proceedings to 40 pages. Preneel points out that for a minority who still want paper proceedings, such an increase will be cumbersome.

A few additional considerations are brought to the table. Ristenpart mentions scalability issues. Preneel recalls that some members publish their top papers at non-IACR venues. Smart notices that in Europe and Asia, in the grander scheme of things, Physics and Biology hold more weight; CS is somewhat of an oddity.

Cachin believes we need to move back to a model where conferences are places to meet people, and journals to credit contribution. He also encourages to have more speakers. Cachin thinks we need to brainstorm more, encourage the membership to discuss, and have another Board discussion by telephone conference. There is consensus that the Board should not decide for the entire membership.

Action Point **11: Cachin and Smart** *(no time set)*:
Come up with a realistic strawman proposal

8. Event reports since last BoD Meeting

8.1. ***Crypto'13.*** Rose (obo Handschuh, GC *C'13*) mentions that *Crypto'13*'s finances (combined with *CHES'13*) look good.

8.2. ***CHES'13.*** Quisquater (SC *CHES*) reports that the conference was a success.

8.3. ***Asiacrypt'13.*** Ling (obo Lokam, GC *AC'13*) has nothing to report.

8.4. ***TCC'14.*** Cachin (obo Halevi, SC *TCC*) reports it took place successfully.

8.5. ***FSE'14.*** Preneel (SC *FSE*) explains that the delay to the post-proceedings of *FSE'13* was due to a problem with a copyright form. It has since been solved. The steering committee continues its support for the system with post-proceedings. The post-proceedings for *FSE'14* are not out yet, but should be soon.

8.6. ***PKC'14.*** Yung (obo Pointcheval, SC *PKC*) reports attendance at *PKC'14* in Buenos Aires was similar as the year before. It was the first IACR event in South America.

9. Forthcoming Conferences

9.1. ***Crypto'14.*** Boldyreva (GC *C'14*) reports that Campbell Hall will not be under construction after all, but it will be used by a welcoming event by UCSB for both Monday and Tuesday morning. If the program chairs decide on parallel sessions, we will be in the University Center for the entire conference. She will prepare a final budget soon.

Benaloh recalls that there will be an overlap with Usenix. Usenix has discussed a joint registration discount. Preneel explains that there is a difference in model, as for Crypto the registration fee primarily covers an attendee's variable costs (essentially food and drinks), whereas for Usenix the registration fee is not derived as directly. The Board refers any decision regarding discounts to Boldyreva, as implementing it might prove difficult.

9.2. ***Asiacrypt'14.*** Ling (obo Guan, GC *AC'14*) mentions that the budget for *Asiacrypt'14* is in the svn. It is a relatively conservative budget at low cost. Sponsorship is looking good. Preneel asks to clarify whether a physical program committee meeting will take place.

9.3. ***Eurocrypt'15.*** Petkova-Nikova (GC *EC'15*) reports that the website is online and the venue has been booked. The Board gives some recommendations regarding contacting sponsors. Cachin thanks Petkova-Nikova.

9.4. ***Crypto'15.*** Ristenpart (GC *C'15*) has nothing to say.

9.5. ***Asiacrypt'15.*** Ling (obo Galbraith, GC *AC'15*) has nothing to add to the written report. Preneel remarks that there will be a minor clash with Thanksgiving.

10. Event proposals, General Chair appointments, and Steering Committee reports

10.1. **Asiacrypt Steering Committee.** Ling has circulated the report via the SVN.

10.2. **Proposal for Asiacrypt 2016.** Duong-Hieu Phan joins the meeting for this item and gives a very clear presentation for a proposal to hold *Asiacrypt 2016* in Hanoi, Vietnam. He confirms that there is a good opportunity to accommodate a larger number of talks using parallel sessions.

Cachin thanks Phan for the work that went into the preparation of this proposal.

The Board unanimously accepts the proposal.

Decision 8. *Asiacrypt 2016 will be held in Hanoi (Vietnam) and Bao-Chau Ngo Duong-Hieu Phan are appointed General co-Chair.*

Duong-Hieu Phan will be taking a seat on the Board.

10.3. **Soliciting a Proposal for *Eurocrypt'16*.** Cachin mentions that there is no concrete proposal yet. Several new people have been contacted, but prefer to bid for 2017. There are several teams that have organized before and would be willing to organize again.

10.4. ***CHES* Steering Committee.** Quisquater (SC *CHES*) gives an update on *CHES'14*. It will be colocated with PROOFS and FDTC. There are several new sponsors. The review process is going smoothly. Preneel remarks that the budget still contains a high cost for internet access.

Quisquater presents an proposal for *CHES'15*. The Board unanimously accepts the proposal.

Decision 9. *The Board approves the CHES'15 proposal, meaning that CHES 2015 will be held in Saint-Malo (France) with Emmanuel Prouff, Guénael Renault, and Matthieu Rivain as General co-Chairs and Helena Handschuh and Tim Güneysu as Program co-Chairs.*

10.5. ***FSE* Steering Committee.** Preneel (SC *FSE*) presents a proposal to hold FSE in Turkey in 2015. The budget has a conservative amount of sponsorship. Preneel believes it to be a reliable proposal.

The Board unanimously accepts the proposal.

Decision 10. *The Board approves the FSE 2015 proposal, meaning that FSE 2015 will be held in Istanbul (Turkey) with Hüseyin Demirci as General Chair and Gregor Leander as Program Chair.*

10.6. ***PKC* Steering Committee.** Yung (obo Pointcheval, SC *FSE*) remarks that *PKC'15* has already been approved by the Board. It will be in the NIST building and will be co-located with PQC. Rose remarks that the location means that non-US citizens will have to register well in advance.

Yung refers to the *PKC'16* proposal on the svn. Preneel remarks that the budget uses the old model, but reckons that the required changes will more or less cancel each other out.

The proposal is approved unanimously.

Decision 11. *The Board approves the PKC 2016 proposal, meaning that PKC 2016 will be held in Taipei (Taiwan) with Chen-Mou Cheng as General Chair and Pino Persiano and Bo-Yin Yang as Program co-Chair.*

The steering committee has already solicited proposals for *PKC 2017*.

10.7. ***TCC* Steering Committee.** *TCC'15* has already been approved.

11. Program Chair and other appointments

11.1. **Program and General Chair List Maintenance.** Cachin very quickly explains the procedure. 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.

Lysyanskaya mentions that she has several people to add to the first timers, as well as people who have served but might come from underrepresented. The first timers will be added, the others not as it will harder to maintain and lead to a less clear message to the chair, plus too much interference.

11.2. **Crypto'15–'16.** Rosario Gennaro has already been appointed as one of the co-chairs for *Crypto'15*. Several excellent candidates are nominated, and after discussion a candidate is selected.

Decision 12. *Matt Robshaw is appointed Program Chair (rolling co-chair) for Crypto'15 and Crypto'16. [Matt Robshaw subsequently accepted.]*

11.3. **Asiacrypt'15–'16.** Tetsu Iwata has already been appointed as one of the co-chairs for *Asiacrypt'15*. Several excellent candidates are nominated, and after discussion a candidate is selected.

Decision 13. *Jung Hee Cheon is appointed Program Chair (rolling co-chair) for Asiacrypt'15 and Asiacrypt'16. [Jung Hee Cheon subsequently accepted.]*

12. Closing Matters

12.1. **Draft Agenda for Membership Meeting.** Cachin remarks that there are no plaques for Fellows for Eurocrypt, but he will announce the Fellows at the membership meeting.

He quickly recapitulates the main issues to discuss at the membership meeting:

- A strawman proposal of a 40 page limit for submissions and publications, excluding the JoC.
- The Board's decision to keep track of gender statistics.

12.2. **Review of Action Points.** After skipping a review of action points, Cachin closes the meeting at 18.12.