MINUTES IACR BOARD MEETING *CRYPTO'13*

UCSB, 18 AUGUST 2013

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 19 attendees, holding a further 6 proxies.

Attendees (Elected). Michel Abdalla (Director –2015); Josh Benaloh (Director –2014); Tom Berson (Director –2015); Christian Cachin (Vice-President –2013) Shai Halevi (Director –2014, TCC Steering Committee); Mitsuru Matsui (Director –2013, delayed arrival, proxy Preneel); 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 –2014); Martijn Stam (Secretary –2013).

Attendees (Appointed). Alexandra Boldyreva (GC *Crypto'14*); Matt Franklin (Journal Editor-in-Chief –2014); Helena Handschuh (GC *Crypto'13*); Aggelos Kiayias (GC *Eurocrypt'13*); Satyanarayna Lokam (GC *Asiacrypt'13*);

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

Absentees (Elected). Anna Lysyanskaya (Director –2015, proxy Halevi);

Absentees (Appointed). D.J. Guan (GC *Asiacrypt'14*); Gregor Leander (GC *Eurocrypt'14*, proxy Paar); Christopher Wolf (Newsletter Editor –2014, proxy Paar). abhi shelat (Membership Secretary –2014, proxy Halevi);

Absentees (Representatives and Others). San Ling (Asiacrypt Steering Committee, proxy Preneel); Jean-Jacques Quisquater (CHES Steering Committee, proxy Paar).

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

1.3. **Action Points.** Preneel briefly reviews the status of action items identified from the *Eurocrypt'13* meeting. Several items are still ongoing and will be retained (in slightly different formulations) and with updated due dates.

(1) (Implementation of new publication contract) This has been done, however the explanatory guideline written by Preneel is not yet easily available to members on the website.

> Action Point **1: Smart** *(18 August 2013)*:
> Add the publication guidelines to the website.

(2) (Discussion Forum) The eprint's discussion forum has been used for the ongoing discussion regarding the future of IACR's publication model. From a technical perspective, this seems to be working, although some voice concern that the discussion is not yet as inclusive as they had hoped for.

(3) (List of committee membership) Stam has created a draft, which is currently only posted on the Board's svn. The Board suggests several corrections and additions and requests the content to be made available online.

(4) (Conference budget template) Still ongoing.

> Action Point **2: Rose** *(1 November)*:
> Update the conference budget template to deal better with student stipends and free attendees.

(5) (Update PC guidelines) Still ongoing.

> Action Point **3: Stam** *(1 September 2013)*:
> Add the bandwidth and balance expectations to the PC guidelines.

(6) (1 Page summary of PC changes) Benaloh has written the summary, but it has not yet been made available online yet.

> Action Point **4: Benaloh** *(1 October)*:
> Make the PC summary available online

(7) (Board guidelines) Still ongoing.

> Action Point **5: Preneel** *(1 November 2013)*:
> Think about the tasks that the officers and appointed directors have to perform.

(8) (Video archiving) Still ongoing.

> Action Point **6: McCurley and Cachin** *(1 August 2013)*:
> Find somebody responsible for overseeing consistency of the recording and archiving of videos of presentations at IACR events.

(9) (Archiving guidelines) Still ongoing.

> Action Point **7: Cachin and Stam** *(31 Augustus 2013)*:
> Archive the audit committee document and the board voting guidelines.

(10) (Updating e-voting guidelines) Benaloh reports this has been done.
(11) (Increasing awareness of ethics) Still ongoing.

> Action Point **8: Ethics Committee** *(31 August 2013)*:
> Increase awareness of ethics by writing a news item on the official announcement channel.

(12) (Photo Archiving) Still ongoing.

> Action Point **9: Orman and Stam** *(1 September 2013)*:
> Make a policy on what (photos etc.) the IACR should archive and how, including dealing with permissions.

(13) (Plagiarism) Orman has discovered the problem is more severe than she initially thought. It would require further Board discussion.
(14) (Bylaws Change) Preneel has uploaded a document.
(15) (Publication Pipeline) Done.
(16) (Authentication System) Still ongoing.

> Action Point **10: Cachin and shelat** *(30 November 2013)*:
> Look at the authentication system used for conference registration etc.

(17) (JoC Web-based System) Franklin reports the transition is in progress.
(18) (JoC Springer Discussion) Still ongoing.

> Action Point **11: Preneel** *(1 October)*:
> Speak to Springer to adapt the Journal contract so it will support our intended infrastructure.

(19) (IACR Statistics) Ongoing, although it has come to light that some statistics are more contentious then we thought.

> Action Point **12: Cachin, shelat, Smart** *(31 August 2013)*:
> Determine which information and statistics IACR should publish online and where.

(20) (PC Reports) Still ongoing.

> Action Point **13: Benaloh** *(no time set)*:
> Chase program chairs for reports.

(21) (Eprint Open Access) A new policy has been implemented.
(22) (Strawman Proposal Slides) Smart has created these.

1.4. ***Crypto'13* Status.** Handschuh (GC *C'13*) reports that there are well over 400 attendees. Roughly a third of the attendees will also attend CHES. The colocation was somewhat complicated as the admin system is not tailored to it. It also turned out that UCSB was not in a position to host joint evening events, primarily due to capacity issues.

There are 26 student speakers with IACR stipends and thanks to our generous sponsors there were additional travel stipends. Handschuh has written 30 visa applications, but unfortunately at least 8 applicants were unable to attain a visa in time. These were typically asked for in early June. See also Agenda Item 12.3.

Preneel thanks Handschuh for her hard and excellent work for a difficult job.

2. Officer's Report for Approval

2.1. **Treasurer's Report.** Rose has sent out the balance figure sheets. The accountant is preparing the tax returns and a small surplus is foreseen.

There is a suggestion to extend the IACR student speaker stipend program to the workshop.

Preneel recalls the Eurocrypt'13 membership meeting, where a small majority was in favour of a fee reduction to take into account reduced costs due to decreased shipping of the Journal.

The Board thanks Rose for doing an excellent job.

3. Guidelines for Approval

3.1. **Evoting Guidelines.** Benaloh has made guidelines to describe for an Election Committee how to operate Helios.

3.2. **General chair guidelines.** Rose remarks that McCurley has made a change to the guidelines to incorporate some advice on making video recordings of the conference presentations.

3.3. **Program chair guidelines.** Benaloh has an updated version of the guidelines, but has not yet distributed it.

3.4. **Audit Committee and Board Voting.** This is an ongoing action item.

4. Appointees Reports for Information

4.1. **Newsletter.** Preneel remarks that Wolf is very pro-active.

4.2. **JoC Editor in Chief.** Franklin is going forward with negotiations for a three-year contract (for a web-based submission system). He remarks that the costs will be at least 5 kUSD, as in addition to fixed costs, there will also be a fee per submission.

Preneel thanks Franklin for his valuable efforts.

4.3. **Archivist.** Orman has provided a detailed report on the current state of the archive. It is still difficult to get the required files from program chairs.

There is an issue about unicity of titles, as there can be minor grammatical differences, as well as issues related to character encoding and representing mathematical formulae. This occassionally causes a discrepancy between the archive and cryptoDB, for instance.

Preneel thanks Orman for her hard work.

4.4. **Membership Secretary.** Preneel (obo shelat) says that overall membership figures are stable.

4.5. **Database and Website.** McCurley has received metadata from Springer and has distributed a small summary during the meeting.

> Action Point **14: Preneel** *(1 October 2013)*:
> Clarify with Springer which rights IACR has regarding to the metadata as provided by Springer, specifically the abstract.

McCurley mentions that the capture of video has created a rapid increase of data, which will have to be taken into account when upgrading IACR's IT infrastructure.

> Action Point **15: McCurley** *(1 October 2013)*:
> Publish a news item asking for volunteers to edit video material (e.g. TCC) to a suitable format.

5. Internal Committee Reports for Information

5.1. **Fellows Committee.** Preneel says there are seven new Fellows, who all, except Lars Knudsen, have elected to receive their plaque at *Crypto'13*.

5.2. **Publication and Web Infrastructure.** See Agenda Items 12.1 and 12.2 for the continuing strategic discussion on the future of publications.

5.3. **Ethics Committee.** Cachin has nothing to report. The irregularity mentioned by the Crypto'13 program chairs has not yet appeared on his radar.

There is a brief discussion how the communication between program chairs and the ethics committee can be improved.

5.4. **Election Committee.** The committee will meet immediately after the Board meeting to determine the Chair and Returning Officer. [Benaloh will be Chair and Abdalla will be Returning Officer.]

5.5. **JoC web system evaluation.** Nothing to report.

5.6. **Journal of Cryptology EiC search committee.** Preneel mentions that the search committee has not yet met.

6. Appointments

There are no appointments to be made for sub-committees of the Board.

7. Conferences since last BoD Meeting

7.1. ***Eurocrypt'13.*** Kiayias gives a brief overview of *Eurocrypt'13.* He has posted videos of all the talks on a private YouTube channel. Roughly half of the authors have used the new IACR form granting IACR permission to make the video publicly available.

There is a discussion on whether authors of early conferences in 2013 should be asked (by their respective program chairs) to sign the new copyright form. Relatedly some ideas to modify the IT flow are mentioned.

Kiayias is thanked for his excellent job.

Action Point **16: shelat** *(1 November 2013)*:
Investigate the user-friendliness of the registration software and draft a proposal (including budget) of recommended changes to aid general chairs.

8. Forthcoming Conferences for Information

8.1. ***Asiacrypt'13.*** Lokam (GC *AC'13*) reports that a very good venue has been found. Registration will soon open. There are plans to have a workshop on the day of the reception, likely on lattice-based cryptography. Due to an increased number of accepted papers, there will be no free afternoon.

Smart observes that program chairs are very reluctant to move to parallel sessions. Preneel will bring the possibility of parallel session up at the membership meeting.

Decision 1. *The Board strongly suggests to the Crypto'14 program chairs to incorporate parallel sessions if the number of accepted papers is high.*

8.2. ***Eurocrypt'14.*** Preneel (obo Leander, co-GC *EC'14*) says preparation for the conference is on track.

8.3. ***Crypto'14.*** Boldyreva (GC *C'14*) mentions that Campbell hall (usually the main venue) is likely to be renovated and unavailable for *Crypto'14*.

8.4. ***Asiacrypt'14.*** Preneel (obo Juan, GC *AC'14*) says preparation for the conference is on track.

9. Steering Committee Reports and Workshop Proposals

9.1. ***TCC'14* Status.** Halevi says there are no new developments; *TCC'15* will be decided upon by the steering committee later in the year.

9.2. ***FSE'14* Status.** Preneel (SC *FSE*) reckons that the venue (the National History Museum in London) will be amazing.

9.3. ***PKC'14* Status.** Pointcheval (SC *PKC*) reports that *PKC'14* is on track. The steering committee has recently received a proposal for *PKC'15* to be organized at NIST (USA).

9.4. ***CHES'13* and *CHES'14* status.** Paar (obo Quisquater, SC *CHES*) reports that *CHES'13* had a very high number of submissions. For the second year there was an author rebuttal phase which people seem to be happy with. There are almost 380 attendees, roughly half of which will attend Crypto as well. The colocation with Crypto will mainly be exploited by joint invited talks. There will be tutorials and industry support is very good.

CHES'14 will be held in Korea.

10. Conference Proposals for Discussion/Selection

There are no proposals to discuss or select.

11. Conference Chairs

11.1. **Program Chairs Reports.** Benaloh reports that everything is going well. The Crypto co-chairs suggested not to allow PC members to submit papers in future. The Board is aware of the delicate matter of PC-authored submissions (and accepted papers), yet for each conference, it is up to program chairs to set the exact rules related to PC submissions.

11.2. **Program and General Chair List Maintenance.** 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.

11.3. **Eurocrypt'15–'16.** Elisabeth Oswald 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 2. *Marc Fischlin is appointed Program Chair (rolling co-chair) for Eurocrypt'15 and Eurocrypt'16. [Fischlin subsequently accepted.]*

11.4. ***Crypto'15* General Chair.** Several excellent candidates are nominated, and after discussion a candidate is selected.

Decision 3. *Thomas Ristenpart is appointed General Chair for Crypto'15. [Ristenpart subsequently accepted.]*

11.5. **Asiacrypt 2015 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 4. *Phil Rogaway is invited to deliver the Distinguished Lecture at Asiacrypt'15. [Rogaway subsequently accepted.]*

12. Strategy

12.1. **Future of IACR Publications.** Smart gives background on the strawman proposal, which is specifically meant to elicit discussion (although the proposal has only recently been made available to a wider audience). Some key design choices:

- A single version of each published paper.
- A unified publication pipeline, where papers do not get reviewed repeatedly.

The two main concerns:

- What does refereeing the full version mean? Would it lead to an increase in reviewing load?
- Should the workshops be included or not? The answer partially depends on the role of workshops: should they be held to the same standard as conferences (but with a more focussed scope) or not? Preneel remarks that ultimately the decision for workshops to join any new model or not is up to the respective steering committees, not the Board (or the membership).

There is significant discussion within the Board on the proposal. The summary below is restructured based on the key questions.

Initial remarks. Halevi has been talking to many people about the proposal and, despite his strong personal misgivings, he heard positive sounds, also on the *TCC* SC.

Halevi (obo Lysyanskaya) mentions an alternative model, where every IACR event will be matched by a special issue of the JoC (with roughly 20 percent of the papers appearing). The program chairs would serve as guest editor. This does result in multiple versions of the same paper, but Halevi does not see this as a problem.

Preneel brings into focus that for explicit, event-driven special issues of the JoC there is a danger that ISI will withdraw indexing. Berson notices that in the past there were special issues, which was an emergency measure to aid indexing (as the pipeline was clogged and resulted in irregular publishing). Rose believes the relevance of the ISI model is dwindling. McCurley brings to the fore his document on publishing, which advocates a single version only (preferably with immediate gold open access) for increased impact (diffusion of citations is a serious issue).

Being cryptologists, it is worthwhile considering any model from an adversarial perspective: for instance can authors abuse the (single-version) system by making small changes?

Full versions. At stake are the obligations on authors to support their work and, relatedly, what reviewers should do with this material. Different parts of our community have different standards. For comparison, in Economics all the data has to be submitted (McCurley). Papers in Nature often have links to appendices and enrichment material that in print would be less useful but provides an opportunity for independent verification.

In cryptology, for implementation or cryptanalytic papers there is currently no requirement to submit programs or source code, although Preneel notices that within the FSE community there is an increased awareness to publish the tools (with the caveat that some cryptanalysis is theoretical as practical resources are insufficient).

A lively discussion on the value of proofs in theoretical papers and full versions in general ensues. There is no consensus within the Board on whether full proofs should be published or not.

On the one hand, it is argued that, from a mathematical perspective, proofs are published and theorems serve only as summaries, so publishing a theorem without a proof is baffling (McCurley). Even a few papers without proofs might tarnish a venue's reputation when compared to other fields (Smart).

On the other hand, Halevi values the ability to write a framework paper only. He argues that the liveliness of our field is largely a result of the model of allowing sketches without instantly weeding out all mistakes. He believes that fleshing out formal proofs in full versions would not materially increase rigour as authors will already be convinced by the proof and he wonders who would be intererested in reviewing and reading all these proofs. He believes the workload on both writing and reviewing papers would increase dramatically to deal with non-interesting parts. He wonders who would be providing detailed reviews.

Preneel observes that the strawman proposal does not exclude the possibility of submitting a 16-page paper with proof sketches only, provided a full version is not uploaded elsewhere. Kiayias notices that a disadvantage of authors relying on proof sketches is that reviewers can spend a lot of time to reconstruct an actual proof (in order to gain sufficient confidence in the result).

Boldyreva favours full versions, where the emphasis should be on rigour and not on length per se. Cachin remarks that in other fields there are separate publication options depending on length. Moreover, the length of the paper is determined by how best to present the work, not by restrictions imposed by the publication venue. Another idea (due to Lindell) is to penalize people who do not have a full version at the time of the conference presentation.

Reviewing load. There appear to be a lot of complaints from the community about resubmissions and the reviewer's workload. Benaloh notices that delays in reviewing are often more a result of not reviewing for a while than of the overall time it takes to review. Two orthogonal suggestions are proposed, namely to have two round reviews within an event (as used for CHES recently) and to pass reviews on from event to event in case of resubmission.

Paar thinks multi-round reviewing will improve papers.

Preneel notices that currently the deadline rush creates many submissions that have not been proofread, which puts an undue burden on the reviewers. Halevi (obo Lysyanskaya) notices that deadlines have an energizing effect; one suggestion (due to Canetti) is to force submissions to be added to eprint at the time of submission (e.g. anonymously under embargo, with the anonymity lifted once the paper is published).

Halevi suggests to pool reviews, where authors on submission have to state whether the paper is fresh or resubmitted. In the latter case, authors should make the reviews (with rebuttal) available as well. On the other hand, Boldyreva thinks having a fresh view can be a good thing.

Conclusion. At least three different goals are identified that the proposed review system attempts to achieve:

- increasing scientific integrity;
- political advantage of the field (an image of scientific integrity);
- making the reviewing system more efficient.

The allocation of papers to a presentation venue is a huge change and implementing the strawman (or a similarly ambitious) proposal will be a hard and potentially destabilizing change process: people might leave the community and there is no guarantee of indexing. While the Board is aware that an aggressive schedule is needed for radical change, it is not up to the Board to simply make an executive decision that could change the field. Something as radical as the strawman proposal should be presented with good justification and decided upon by the membership (e.g. to prevent a backlash against such a centralized system).

Smart reiterates the huge benefit of the new model when comparing to other fields. We want to make the field more mature, but there are several orthogonal choices to be made. Halevi asks whether Smart could deconstruct the proposal into orthogonal components: What are the key questions to ask to the membership?

McCurley compliments Smart on surfacing a lot of fault lines within the community with his proposal, and believes we still might agree on a number of goals. Preneel suggests people start discussing and invites people to come up with alternative strawman proposals. Feedback from the respective Steering Committees will need to be solicited.

12.2. **ICT Infrastructure.** Preneel recalls that the IACR currently has a fairly large number of IT systems (to deal with publications, eprint, conference registration, the website) that are in need of revision. The website and conference registration are largely independent systems.

Revision of the website is still in progress, for instance a discussion board and upgrading the hardware are planned (a new disk may be purchased) Cachin comments that it would be good to have a web design that is more interactive, making it easier for other people to post. If we would move to a content management system (CMS) even people without access to the relevant files on the server could contribute. The problem is that a CMS tends to assume control over the whole website, which might be undesirable.

Action Point **17: Cachin (lead), McCurley, Wolf, Smart** *(no time set)*:
Clean up the website

McCurley wrote a discussion document focussed on the publication process. The Board has just decided for an option to support the Journal of Cryptology; for the conferences any update will partly depend on the outcome of the publications discussion.

Cachin wonders how the e-library will be integrated with the rest of the website. McCurley thinks an integrated system would be good, and we should hire someone to develop the project. He volunteers to manage this developer (but not whomever will subsequently administer the publication process), for instance to ensure proper documentation is written for future maintenance.

12.3. **Visa Problems for Attending Events in the USA.** Halevi reports on several recent cases of people who had difficulty in obtaining timely visas and would like the Board to get a clearer picture of the problem. Getting accurate information on who submitted when and where is difficult. Smart mentions that three people from Bristol got delayed and that this delay seemed triggered by mentioning that they were going to Crypto. This might indicate a change in attitude recently (another factor is that the sequestor will have reduced available government manpower).

Preneel notes that in the past, the IACR has asked the State Department or the National Science Foundation for advice, and he suggests to do so again.

Action Point **18: Preneel and Berson** *(no time set)*:
Write a letter to the NSF and/or State Department concerning US Visa applications.

12.4. **Policy on Responsible Disclosure and Publications.** Preneel brings to mind Ross Anderson's recent email concerning security-related research whose publication was prevented as a result of legal action. Anderson suggested to publish papers before acceptance to thwart legal interference of academic research. Rose observes that responsible disclosure requires contacting the vendor ahead of publication and Orman notices that the legal system can still pressure the author to take down a paper.

Preneel has been in contact with Paterson who has read most of the case documents. However, since this is not an IACR publication and it is unlikely that any of the authors is an IACR member, the IACR is currently not in a position to comment on this particular case. Preneel did however find a statement written in 1997 by the IACR Board (specifically McCurley) on Research Publication Policy. The statement is still relevant and could be posted publicly.

12.5. **Life Membership.** Preneel presents a proposal to introduce life membership for senior members of our community. There is some discussion whether, in the long run, this might result in a large number of retired members. A change in the Bylaws should allow the Board to reinstate a fee for senior members.

With 1 abstention and the remaining votes in favour, the Board decides to:

Decision 5. *Instigate a change to the Bylaws related to senior membership to put forward for a vote to the membership this year.*

Benaloh wonders whether we should change the Bylaws to enable the Board to void certain memberships in case of incidents.

12.6. **Sponsoring of Summer Schools.** Abdalla mentions the success of eCrypt summer schools, but unfortunately eCrypt funding has run out. These schools would address hot topics, targeted at graduates. The question is whether the IACR would be willing to support such schools financially and if so, how to implement such support. Various aspects are raised regarding to IACR's level of involvement and how we would decide which schools to support. There is already a request from a potential summer school in Romania.

Support of schools in general is well-received and would fall within the remit of the IACR. However, a clear policy and good governance of it leading to a transparent process are needed. This amounts to significantly more work than writing cheques and support of a subcommittee to help run the summer school program is called for.

One suggestion is to capture lectures on video (as criterion for funding) to enable wider dissemination. In first instance, a decent policy needs to be written, to be done by the Seasonal School Committee.

Decision 6. *Michel Abdalla, Greg Rose, Alexandra Boldyreva, Aggelos Kiayias and Lin Sang are appointed to the Seasonal School Committee.*

Action Point **19: Seasonal School Committee** *(1 October 2013)*:
Write a draft policy (in LaTeX) regarding IACR's support of Seasonal Schools.

12.7. **Composition of the Board.** The Bylaws do not mention the Steering Committees and there are various roles that are no longer relevant or existing. For instance, the Newsletter Editor could be rephrased in Communications Secretary. Cachin mentions that the Bylaws could include a way to add further appointees or non-voting attendees, where voting rights would have to be discussed. Legally it is unclear whether appointees are even allowed to vote on fiduciary issues (which could include decisions on general chairs), and legal advice should be sought.

Decision 7. *Instigate a change to the Bylaws (Article 5), to put forward for a vote to the membership this year, so that the Board at its discretion may appoint a limited number of additional non-voting members to the Board.*

Action Point **20: Preneel** *(no time set)*:
Take legal opinion on who can vote in the Board.

13. Closing Matters

13.1. **Draft Agenda for General Meeting of Members.** Preneel quickly recapitulates the main issues to discuss at the membership meeting.

- Parallel Sessions
- Future Publications
- Change of Bylaws

13.2. **Review of Action Items.** After a brief review of action points, Preneel closes the meeting at 17.51.

14. Intermediate Board Decisions

Decision 8 (11 November 2013). *The Board approves the PKC 2015 proposal, meaning that PKC 2015 will be held at NIST (Gaithersburg, near Washington D.C.) with Rene Peralta as General Chair and Jonathan Katz as Program Chair.*

Decision 9 (11 November 2013). *Ivan Damgård is appointed Editor in Chief of the Journal of Cryptology for the period 2014–2016.*

Note that this means that the EiC Search Committee has done its job and is disbanded. In 2014, Franklin and Damgård will share the role of Editor in Chief to allow for a smooth transition.

Decision 10 (21 December 2013). *The Board approves the TCC 2015 proposal, meaning that TCC 2015 will be held in Warsaw (Poland) with Stefan Dziembowski as General Chair and Yevgeniy Dodis and Jesper Buus Nielsen as Program co-Chairs.*

Following his election as Vice-President, Nigel Smart relinquished his post as Elected Director (which would last until 31 December 2014) from 1 January 2014. The Bylaws require the President to appoint a replacement, to be approved by the Board.

Decision 11 (19 January 2014). *Moti Yung is appointed as Elected Director for the one-year term of 2014.*

Decision 12 (30 April 2014). *The creation of IACR Cryptology Schools and the Policy for Cryptology Schools are approved.*

Note that this means that the Seasonal School Committee has done its job and is disbanded.

Decision 13 (30 April 2014). *Michel Abdalla (chair), Masayuki Abe, Alexandra Boldyreva, Aggelos Kiayias and Moti Yung are appointed to the 2014 Schools Committee.*