MINUTES IACR BOARD MEETING *CRYPTO'15*

UCSB, SANTA BARBARA, 16 AUGUST 2015

1. Opening Matters

1.1. **Welcome, roll of attendees, identification of proxies.** At 10:04 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.

1.1.1. *Roll of Attendees.* There are 19 attendees, holding a further 4 proxies, and an observer joining for shorter stretches.

Attendees (Elected). Michel Abdalla (Director –2015); Masayuki Abe (Director –2017); Josh Benaloh (Director –2017); Tom Berson (Director –2015); Christian Cachin (President –2016) Anna Lysyanskaya (Director –2015, proxy Yung); Christof Paar (Director –2016, *CHES* Steering Committee); David Pointcheval (Director –2016, *PKC* Steering Committee); Bart Preneel (Director –2016, *FSE* Steering Committee); Greg Rose (Treasurer –2016); Nigel Smart (Vice-President –2016); Martijn Stam (Secretary –2016); Moti Yung (Director –2017).

Attendees (Appointed). Brian LaMacchia (GC *Crypto'16*); Thomas Ristenpart (GC *Crypto'15*); Mike Rosulek (Communications Secretary, –2016).

Attendees (Representatives and Others). Hilarie Orman (Archivist); Yu Yu (Webmaster).

Attendees (Observers). Xuejia Lai (*Asiacrypt* Steering Committee); Gilles Brassard (chair of Fellows committee, item 3.1).

Absentees (Elected). None.

Absentees (Appointed). Ivan Damgård (Journal Editor-in-Chief –2016, *TCC* Steering Committee, proxy Cachin); Steven Galbraith (GC *Asiacrypt'15*, proxy Smart); Svetla Petkova-Nikova (GC *Eurocrypt'15*, proxy Preneel); Krzysztof Pietrzak (GC *Eurocrypt'16*); Phan Duong Hieu (GC *Asiacrypt'16*, proxy Abdalla). abhi shelat (Membership Secretary –2014).

Absentees (Representatives and Others). Kevin S. McCurley (Database Administrator).

1.2. **Review and approve agenda.** The agenda is approved with some minor changes.

1.3. **Action Points.** Cachin briefly reviews the status of action items identified from the *Eurocrypt'15* meeting.

(1) shelat has implemented the JoC opt-in system; around 45 people have opted in. There is a small glitch as a result of which people might not have to pay yet.
(2) Berson responds that the audit committee has not done a full audit yet. The plan is to do a full audit of the 2014 financial year in October/November.
(3) The rump session has not taken place yet; Stam will contact Damgård.
(4) The PC reports have not been migrated to the SVN yet.
(5) This item is considered done.
(6) Yu Yu has taken up the PhD database.
(7) The guidelines have been updated, but further discussion will take place today.
(8) Smart remarks that it is beneficial to appoint the Ethics committee 2016 already today rather than waiting until *Eurocrypt'16*. Berson remarks he will not be running on the Board again, and will not be available for continued service on the Ethics committee. Cachin thanks Berson for his long service on the IACR Board.

Decision 1. *Smart (ex officio), Benaloh (as Programme Chair Liaison), and Pointcheval are appointed to the Ethics Committee for the 2016 calendar year.*

The remaining action points are all taken care of; some will be discussed later during the meeting.

1.4. ***Crypto'15* Status.** Ristenpart (GC *C'15*) says everything is going on track. The number of accepted papers is 76; there are parallel tracks for the program. According to the latest budget, there will likely be as slight overspend. The number of registrations is around 315, roughly 20% of whom are students. This means that overall registration is a bit lower than in previous years. A few people had problems obtaining a visa.

Cachin thanks Ristenpart for his hard work.

2. Officer and Appointee Reports

2.1. **Treasurer's Report.** Rose reports that financially IACR is healthy. He gives some further information on how the CRI Endowment has been spent. So far 4 schools at 5k each plus a large number of stipends for student speakers at conferences and workshops have been awarded.

> Action Point **1: Abdalla, Benaloh, Berson, Cachin, Handschuh, Rose** *(no time set)*:
> The endowment committee should meet.

For those not at the *Eurocrypt'15* Board meeting, Rose explains some of the difficulties he has had transferring money to India, as well as some problems related to hosting a conference at NIST.

The audit committee has not been very active yet; the Board will ask the committee to report at *Crypto'16*.

Cachin thanks Rose for his hard work.

2.2. **JoC Editor in Chief.** Cachin has not yet received a report from Damgård.

2.3. **Program chair reports (+Ethics Committee).** Benaloh has not received any program chair reports. The Ethics committee has dealt with a triple submission, but it will keep the author name(s) anonymous. However, it will continue to liaise with Program Chairs.

2.4. **Communications Secretary (Petitions, website, etc.)** Rosulek responds that we have a new domain ia.cr and a facebook page. Cachin asks how the facebook page is integrated with for instance our news system and the IACR Twitter feed. Currently Rosulek manually takes care of synchronisation.

The website has been updated to enable petitions; the petition regarding Australia's proposed legislation relating to cryptology has been signed by over two hundred members. Smart wants to mention the petition to the membership.

A discussion ensues to what extent petitions are political and what this implies to IACR's role. Orman recalls that in the early days, researchers would receive warning letters. Berson elaborates that at the first *Crypto*, it was not even clear whether the meeting would go through or whether it would be deemed illegal.

Yung and Rose believe the IACR's mission has a political component, emphasizing the I is for International and the R for research. Rose clarifies that the IACR is allowed to be political under current tax rules, which extends to spending money; we cannot however be partisan. The Board believes that the IACR should try to argue based on professional values, acknowledging the clear political dimension.

Regarding the process, LaMacchia draws attention to IACR's relatively slow decision making process when it comes to taking up a position as organisation. He wonders whether we can clarify and streamline the processes to ensure low latency, making a distinction between what we decide as Board, what the membership endorses (e.g. petitions and motions), and what the IACR funds. LaMacchia suggests partnering with NGOs in some cases, although he is wary this might infringe corporate space.

Lysyanskaya feels that in order to have a petition, there should be clear majority within the Board. Preneel however is not convinced there is a need for a supermajority. In order to reduce latency, Benaloh suggests that a petition can be accepted as soon as two thirds of the Board agree (or otherwise use a simple majority at the cut off date of the vote).

Preneel mentions that additionally a forum could be useful.

Cachin thanks Rosulek and Yu for their great work.

2.5. **Membership Secretary.** Following *Eurocrypt'15*, Cachin has had a discussion with shelat, who has indicated that he would like to continue as membership secretary (formally his term expired end of 2014). He has done a lot of work on the updates. Rose believes shelat is doing a good job.

The overall system still needs to be redesigned as there is currently little integration between the membership database, eprint, websubrev and Springer (for instance for canonical names). Stebila has done some preliminary work on reimplementing the eprint archive in the past, but progress on it has stalled.

Decision 2 (Unanimously)**.** *shelat is appointed as membership secretary for 2015–2017.*

Cachin (obo shelat) report that there are about 1400 members at the moment.

2.6. **Archivist.** Orman reports that the Archive is up to date as far as allowed by our contract with Springer. There is still a communication problem with Springer related to obtaining meta-data to populate CryptoDB and the Archive. Obtaining (source for) the front matter is still a point of contention.

> Action Point **2: Smart** *(no time set)*:
> Talk to Robshaw to see exactly how front matter for proceedings is generated.

Orman remarks that Diffie has obtained various retypeset, electronic copies of historical articles, such as Shannon's seminal paper. Currently, there is no good mechanism for making these papers available. Cachin believes a historical bibliography could be used, possibly making available the source as well. Orman suggests to add the context of the work as well. Rosulek remarks that author's and copyright holders may deny public posting of some of the material.

> Action Point **3: Rosulek and Orman** *(no time set)*:
> Add a component to the website for a historical archive.

3. Internal Committee appointments, reports, and decisions

3.1. **Fellows Committee.** Cachin wants to discuss two aspects of the Fellowship guidelines. The first suggested change is to allow Fellows (who might not be members) to nominate. This change is accepted without much discussion.

Decision 3. *The terms of the IACR Fellows Program are amended to allow Fellows to act as nominator as well.*

The second point relates to the number of IACR Fellows inducted annually. Brassard (chair *Fellowship Committee*) believes that the recent guideline to promote consistency in the number of IACR Fellows inducted annually was achieved in the wrong direction. He provides two argument: firstly, having many new Fellows in one year dilutes the honour; secondly, and this is a counting argument, we are nearing a situation where 5% of our membership is a Fellow, which was the original target (5% of the current membership equates to roughly 70 Fellows, currently there are 53 IACR Fellows). Brassard believes that in very few years we would reach a situation where the target.

Yung explains that, when the Board discussed the issue last year. the 5% was meant to refer to active Fellows. Cachin suggests to express the annual increment in terms of a percentage of the membership instead of using absolute numbers. Additionally, it is suggested to subsequently forget about the 5% target, in order not to have to model activity or longevity of Fellows.

Decision 4. *The terms of the IACR Fellows Program are amended as by removing the sentence "The target maximum number of Fellows is approximately 5% of the IACR members." and adding "The total number of Fellows to be selected in any one year is expected to be approximately 0.25% and should not exceed 0.5% of the current total membership."*

3.2. **Audit Committee.** The audit committee as it stands needs to be reappointed.

Decision 5. *Tom Berson, Helena Handschuh, and Christof Paar are appointed for the Audit Committee 2016–2018.*

3.3. **Ethics Committee.** The committee has already reported elsewhere.

3.4. **Schools Committee.** Abdalla reports that Yung stayed on after all with Kiaiyas stepping down instead; this has not been reported in full yet. Preneel notices that one of the proposals is within a month, which indicates that our guidelines or procedures might need to tightened. Smart believes that in future we should make a decision three months in advance with submission at least six months in advance. Preneel remarks that we might clarify the guidelines regarding how the recurring nature of a school will influence prioritization.

> Action Point **4: Abdalla** *(no time set)*:
> Update the School Committee guidelines.

Five requests for School funding have been received by the School Committee. Abdalla gives a summary of the Committee's findings and recommendation. The Board decides to fund the two schools as recommended by the School Committee.

Decision 6. *The Board adopts the proposal by the Schools Committee, meaning that the Summer School on Elliptic Curve Cryptology (September 23-25, 2015, Bordeaux, France) will be supported with 5k$ and the Summer School in Cryptocurrencies (May 30 - June 2, 2016, Kos, Greece) will be supported with 10.5k$.*

3.5. **Election Committee.** Benaloh gives an update on the upcoming elections.

4. Program Chair and other appointments

4.1. **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. Especially the first-time PC member list is successfully being depleted by program chairs.

4.2. **Eurocrypt'17–'18.** Jean-Sébastien Coron has already been appointed as one of the co-chairs for *Eurocrypt'17*. Several excellent candidates are nominated, and after discussion a candidate is selected.

Decision 7. *Jesper Buus Nielsen is appointed Program Chair (rolling co-chair) for Eurocrypt'17 and Eurocrypt'18. [Nielsen subsequently accepted.]*

4.3. **Crypto 2017 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. *Shafi Goldwasser is invited to deliver the Distinguished Lecture at Crypto'17. [Goldwasser subsequently accepted.]*

5. Procedures and Guidelines

5.1. **Discussion of needed revisions.** There are no revisions envisioned apart from those separatedly tabled.

5.2. **Non-discrimination policy for GC guidelines.** LaMacchia has prepared revisions to guidelines that clarify the IACR's non-discrimination policy (in particular with respect to academics versus non-academics).

Decision 9. *The new General Chair guidelines and corresponding changes to ICW and Schools guidelines are approved.*

6. Current Publications

6.1. **Publications administrator.** Preneel has prepared a status update on how many author versions of papers are not on the eprint (even after numerous reminders). KU Leuven is still supporting the checking process. It would be good to automate the process (using websubrev), making the authors responsible for updating the (mandatory) footnote.

Smart points out that populating CryptoDB with publications is still problematic.

7. Publications and conference strategy

7.1. **Future publications and publisher.** Cachin recalls the *FSE* Steering Committee's desire to move to a journal based model. Additionally there is an increased move within CS towards Gold Open Access, where the exact published version is available online for free. Currently we have Green Open Access, where authors can publish their version of the paper. Cachin has been speaking with a number of publishers to obtain quotes for Gold Open Access for all publications of the IACR. With an exception for FSE, these quotes from all three publishers are based on the current type and number of publications and assuming similar page lengths. The quotes assume that IACR will be responsible for all payments to the publisher (though internally we may decide on an author's fee). Qualitatively, the quotes differ for long term access (for instance when IACR would move publisher or when the publisher ceases to exist).

Cachin gives all other board members an opportunity to voice their initial thoughts.

There is a remaining question whether the *FSE* steering committee envisions Green or Gold Open Access for their new Journal (taking into account that the JoC has a one year embargo). Preneel clarifies that there is no outspoken preference by the *FSE* steering committee. He also mentions the timeline for *FSE*, where the first CfP (for the new model) will go out in April 2016.

Paar mentions that *CHES* is very happy with Springer; he believes that changing publication carries a substantial reputation cost with you. Paar remarks that he is not clear whether the *CHES* steering committee would be happy with Gold open access given the increased cost. It could redefine the relationship between the Board and the steering committees.

There is an argument how much work self publishing will be, in a way that the resulting publications will be respected by funding agencies, promotion committees, etc. Orman suggest to ask the membership about self-publishing. Preneel and Paar add that for *FSE* and *CHES* self-publishing will not be acceptable.

Smart reiterates that the functionality delta between Green and Gold is fairly small, yet the price differential is significant. Preneel remarks that from a global perspective if everyone moves Gold, eventually the costs for libraries go down. He agrees that the current quotes of 200k$ for Gold are too much, but draws attention that for years we were paying 100k$ on an annual basis to Springer. From that perspective the costs Gold is reasonable.

Rose believes that there is a perception problem in the sense that a lot of costs went down recently, whereas for Gold one would ask for more money without clear benefits. Cachin wonders what we would pay to Springer and what we would be willing to pay another publisher for the service.

Regarding the financial model (who pays), Cachin notices that one reason ACM does not pursue full Gold open access is that for instance patent agencies currently contribute to gain access to papers. This income would be removed in a Gold scenario. LaMacchia questions to what extent we can allocate IACR funds to publication. Rose answers that as Board we should select the best proposal and Yung emphasizes that publications are both for the reader and the writer.

Overall, there does not appear to be enough stomach or momentum to go for Gold. LaMacchia does suggest to see whether the backlog can be released gradually as part of a new contract with Springer.

7.2. **Parallel tracks, review and next steps.** Cachin explains that *Eurocrypt'15* had parallel tracks and it went well, as indicated by various straw polls. There will be a vote among the membership in January 2016. Orman asks whether the ballot would be specifically for two tracks or for parallel tracks in general. Smart notices that Program Chairs might have a problem running more than two tracks due to practical constraints.

8. Event reports since last BoD Meeting

8.1. ***Eurocrypt'15*.** Nikova's (GC *EC'15*) reported that the conference, which for the first time included parallel tracks, went smooth; there were 322 registered participants of whom 99 students. Finally, a substantial surplus is expected. [Due to a communication mishap, this report was not discussed during the meeting.]

9. Forthcoming Conferences

9.1. ***Asiacrypt'15*.** Cachin (obo Galbraith GC *AC'15*) reports that the registration fee is really low thanks to sponsorship.

9.2. ***Eurocrypt'16*.** Pietrzak (GC *EC'16*) is not here to give an update.

9.3. ***Crypto'16*.** LaMacchia has secured his first corporate sponsor. The conference will be at UCSB and colocated with *CHES'16*.

9.4. ***Asiacrypt'16*.** After sorting out some issues, the final contract with the hotel has been lined up. Abdalla suggests to investigate the possibility of having a colocated summer school prior to the conference.

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

10.1. **Proposal for *Eurocrypt'17*.** Abdalla has prepared a bid to host *Eurocrypt'17* in Paris in mid-May. There will be a brief walk between the conference venue and the lunch venue. The Board supports the proposal, but does ask Abdalla to explore options to reduce the registration fee.

Decision 10. *Eurocrypt'17 will be held in Paris (France) and Michel Abdalla is appointed General Chair.*

> Action Point **5: Smart, Stam** *(Eurocrypt'16)*:
> Solicit and coordinate *Eurocrypt'18* proposals.

10.2. **Asiacrypt Steering Committee.** Lai mentions that *Asiacrypt'17* has already been appointed last year.

10.3. ***Crypto'17* General Chair appointment.** Several excellent candidates are nominated, and after discussion a candidate is selected.

Decision 11. *Steve Myers is appointed General Chair for Crypto'17. [Myers subsequently accepted.]*

10.4. ***CHES* Steering Committee.** Cachin reports that there is a budget for *CHES'16*. Preneel has some comments on the budget, plus there still needs to be a discussion with LaMacchia to coordinate joint registrations. Paar will work with the general chairs to revise the budget.

The deadline for proposals of *CHES 2018* is next week.

For the outside, CHES will change its name to a conference (like TCC), but for internal purposes IACR will continue to refer it a workshop (some of this terminology is embedded in the Bylaws). Yung suggests to refer to the current workshops as special area conference.

10.5. ***FSE* Steering Committee.** Preneel (SC *FSE*) notices that the Steering Committee is looking at a proposal for *FSE'17* and the Board should expect details before Christmas.

10.6. ***PKC* Steering Committee.** Pointcheval (SC *PKC*) has nothing further to report.

10.7. ***TCC* Steering Committee.** Cachin has not yet received a proposal for *TCC 2016-B*, although he believes a proposal is under discussion within the steering committee.

11. Closing Matters

11.1. **Draft Agenda for Membership Meeting.** Cachin quickly recapitulates the main issues to discuss at the membership meeting, namely

- Publications (incl. FSE Journal);
- IACR Statements and Petition protocol;
- Feedback on parallel sessions.

11.2. **Review of Action Points.** After a review of action points, Cachin closes the meeting at 18.00.

12. Intermediate Board Decisions

Decision 12 (10 September 2015)**.** *The Board approves the TCC 2016-B proposal, meaning that TCC 2016-B will be held in Beijing (China) with Dongdai Lin as General Chair and Martin Hirt and Adam Smith as Program co-Chairs.*

Decision 13 (15 January 2016)**.** *The Board amends the Bylaws in accordance to the proposal, whereby "General Conference" and "Area Conference" replace what used to be called "IACR Conference" and "IACR Workshop" and "Steering Committees" receive formal standing.*

The (full) amendment was subsequently ratified by a referendum to the members.

Decision 14 (15 January 2016)**.** *The Board approves the FSE 2017 proposal, meaning that FSE 2017 will be held in Tokyo (Japan) with general co-chairs Tetsu Iwata and Shiho Moriai.*

Decision 15 (21 March 2016)**.** *The Board approves the hybrid publication model suggested by the FSE Steering Committee and it gives the President and representatives of the FSE Steering Committee a mandate to negotiate with Ruhr Universität Bochum as publisher of the newly formed IACR Transactions on Symmetric Cryptology.*

Decision 16 (21 March 2016)**.** *The Board approves the FSE Steering Committee's recommendation of Bart Preneel as co-Editor-in-Chief of the IACR ToSC for 2016 and Program co-Chair of FSE 2017 and of María Naya-Plasencia as co-Editor-in-Chief of the IACR ToSC for 2016 and 2017 and as Program co-Chair of FSE 2017 and FSE 2018.*

Decision 17 (21 March 2016)**.** *The Board adopts the proposal by the Schools Committee, meaning that the IACR-SEAMS School on Cryptography (November 24 - December 02, 2016, Hanoi, Vietnam) will be supported with 8k$ and the School on Randomness in Cryptography (August 29 - September 3, 2016, Barcelona, Spain) and the ECC2016 Computational Algebraic Number Theory School (September 1-4, 2016, Izmir, Turkey) will be supported with 5k$ each.*

For the decisions of the 21st of March quoracy was called into question, as there were only 11 yes votes (for each of the proposed decisions). There are normally 22 voting members on the Board, including the President (namely 4 Elected Officers, 9 Elected Directors, 6 Appointed General Chairs and 3 further Appointed Directors), however due to Abdalla's double membership (both as Elected Director and *Eurocrypt'17 Chair*) the effective number of board members is currently 21. For any decision outside a Board meeting, a majority is needed for acceptance (which is 11).