MINUTES IACR BOARD MEETING *EURORYPT'16*

VIENNA, AUSTRIA, 8 MAY 2016

1. OPENING MATTERS

1.1. **Welcome, roll of attendees, identification of proxies.** At 10.03 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 15 attendees, holding a further 6 proxies; three invited guests joined for brief presentations as indicated locally in the minutes.

Attendees (Elected). Masayuki Abe (Director –2017); Josh Benaloh (Director –2017); Christian Cachin (President –2016) Christof Paar (Director –2016, *CHES* Steering Committee); David Pointcheval (Director –2016, *PKC* Steering Committee); Bart Preneel (Director –2016, *FSE* Steering Committee); Phillip Rogaway (Director –2018); Greg Rose (Treasurer –2016); Nigel Smart (Vice-President –2016); Martijn Stam (Secretary –2016);

Attendees (Appointed). Ivan Damgård (Journal Editor-in-Chief –2016); Brian LaMacchia (GC *Crypto'16*); Krzysztof Pietrzak (GC *Eurocrypt'16*); Phan Duong Hieu (GC *Asiacrypt'16*).

Attendees (Representatives and Others). Yu Yu (Webmaster).

Absentees (Elected). Michel Abdalla (Director –2018, GC *Eurocrypt 2017*, proxy Pointcheval); Anna Lysyanskaya (Director –2018, proxy Damgård); Moti Yung (Director –2017).

Absentees (Appointed). Steve Myers (GC *Crypto'17*, proxy LaMacchia); Mike Rosulek (Communications Secretary, proxy Yu); abhi shelat (Membership Secretary –2017, proxy Cachin). S.M. Yiu (GC *Asiacrypt'17*, proxy Pietrzak);

Absentees (Representatives and Others). Kevin S. McCurley (Database Administrator) Shai Halevi (*TCC* Steering Committee); Xuejia Lai (*Asiacrypt* Steering Committee); Hilarie Orman (Archivist);

1.2. **Review and approve agenda.** The agenda is approved as is.

1.3. **Minutes.** Stam apologizes for the lack of minutes of *Crypto'15*. There is a brief discussion regarding the quoracy of the decisions from the 21st of March. The Board ratifies the relevant decisions.

> Action Point **1: Stam** *(20 May 2016)*:
> Update *Crypto'15* minutes.

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

(1) The endowment committee has not yet met, so it should still do so.

> Action Point **2: Endowment Committee** *(July'16)*:
> Meet to discuss strategic use of the endowment

(2) Smart has talked to Robshaw who confirmed that front-matter for conference proceedings is automatically generated from the meta-data in the WebSubRev system. This should suffice for re-generating author-version PDFs for the Archive.

> Action Point **3: Abdalla, Halevi, Orman, Yu** *(Crypto'16)*:
> Figure out how publication metadata gets entered into CryptoDB.

(3) The *Museum of historic papers* has been set up on the website.

(4) In Abdalla's absence, it is unclear whether the School guidelines have been updated.

> Action Point **4: Abdalla** *(July'16)*:
> Update School Guidelines regarding timeline and prioritization of recurring schools.

(5) Done, there will be two *Eurocrypt'18* proposals presented today.

1.5. ***Eurorypt'16* Status.** Pietrzak (GC *EC'16*) says everything is going smoothly. The number of registrations is just slightly fewer than expected. There will be events every evening.

Cachin thanks Pietrzak for his hard work.

2. Officer and Appointee Reports

2.1. **Treasurer's Report.** Rose explains the highlights of the reports he uploaded to the SVN repository. He mentions some of the challenges on keeping reasonable interest rates. He explains that from an administrative perspective and for security reasons, fewer files are kept live on the system, which implies for instance that general chairs will need to stick to deadlines when it comes to closing accounts. Rose briefly describes how last year's conferences did financially. He mentions that Clark has been extremely helpful in the past few years, especially when it comes to European VAT Regulations.

Cachin thanks Rose for his hard work.

2.2. **JoC Editor in Chief.** Damgård (*JoC* EiC) reports that the Journal is operating two pipelines, as Franklin is still handling a fair number of papers on the old system. Since the new system has gone online, the number of "spam" submissions that are summarily rejected has increased. Damgård is looking to appoint a few new members to the Editorial Board. He himself will be stepping down as EiC at the end of 2016 and he expects the new system will facilitate a smooth transition.

2.3. **Program chair reports (+Ethics Committee).** Benaloh mentions that there are a number of program chair reports, but not all. Relating to a discussion about organizing the rump session, the Board confirms the autonomy of program/general chairs in organizing a conference and the Board will support the chairs' decision.

Smart thanks Benaloh for his hard work as PC Liaison.

2.4. **Communications Secretary.** Yu (obo Rosulek) reports their joint activity. The ePrint report pages now support a limited amount of LaTeX. Rosulek requests funding for a re-design of the website, which would involve both the design and the logic behind the site. Cachin supports the idea but mentions that the exact scope of the job is not yet known, and with it the associated costs are still unclear. Smart mentions that especially the conference sites are problematic on mobile devices.

Decision 1. *The Board authorizes the President to spend up to 10k$ on a proposal jointly developed between him and the web-design team.*

Cachin thanks Rosulek and Yu for their great work.

2.5. **Membership Secretary.** Cachin has not yet received a report from shelat. There might be a forthcoming request for development funding. LaMacchia flags that for the membership database maintenance needs to be scheduled carefully to limit the knock-on effects of downtime as much as possible.

3. Publications

3.1. **FSE & IACR ToSC.** Preneel gives an overview of what has been done to introduce the new publication model for *FSE* by introducing the IACR *Transactions on Symmetric Cryptology* (abbreviated *ToSC*). There is a FAQ and a CfP; for the latter there was some discussion on page limits. The schedule is determined, with three deadlines later this year. Work on a LaTeX-style file is still ongoing.

Preneel mentions that the contract with Ruhr Universität Bochum will be fairly short and simple, but on the IACR side we still need to sort out the copyright and licensing situation. There is a discussion whether the author retains the copyright and signs an appropriate creative commons license for IACR to publish through RUB, or whether the author signs over the copyright to IACR, where IACR will then license the work to ensure gold open access. For certain authors, signing over copyright can be easier than getting a CC-BY signed; moreover a CC-BY (either by the author or IACR) still allows others to re-publish for profit.

Action Point **5: Preneel, Cachin, Smart** *(1 July)*:
Draft and decide on a copyright policy for the *ToSC*.

Action Point **6: Preneel, Smart, Yu** *(This week)*:
Figure out where the *ToSC* will be listed on the website (and add to it accordingly).

Cachin notices that the CfP currently uses the terms *FSE* and IACR *ToSC* almost intercheangable. Preneel says the double-branding at this point is deliberate.

The Board thanks Preneel for his hard work.

3.2. **Proceedings & Springer.** Cachin had a conversation with Holman (Springer), where he explained that we would like to remain with Springer in a flexible way, so other IACR Conferences might make a transition to hybrid transactions independent of the duration of the Springer contract.

3.3. **Growing IACR.** LaMacchia notes that Usenix has started a new conference called Enigma, which has invited speakers only. Rogaway mentions that people go there to listen to good talks. Smart explains the backdrop of Real World Crypto. He suggests to create a clearer picture of other workshops to identify communities we are currently not engaging with as much as we could. Rogaway suggests colocating with PETS (which is usually in July); Cachin mentions CSF is considering colocation with Crypto at some point as well.

Abe suggests for the School committee to widen its focus to workshops (without proceedings) as well, especially as the dividing line is not always as clear. Preneel is not sure that adding more Area Conferences is necessarily the best solution; instead we could look at our current events and see how to ensure the General Conferences are more broadly representative, also to non-academics. Rose recalls the lessons learned from Usenix.

Hieu asks about the potential of growing geographically with a stronger emphasis on local communities.

4. Internal Committee appointments, reports, and decisions

4.1. **JoC Editor-in-Chief appointment.** As Damgård will be stepping down at the end of the year as JoC Editor-in-Chief, a new editor is needed.

Decision 2. *The Board appoints Christian Cachin, Phillip Rogaway, and Ivan Damgård, to the Editor-in-Chief search committee.*

Cachin wonders whether an open call for nominations is worthwhile. Preneel says that this might require a formal procedure to avoid for instance potential conflicts of interest. Instead of asking people to apply formally, instead people could make suggestions, with formal applications only to be sollicited by the search committee.

4.2. **Fellows Committee.** Cachin reports on his communications with Brassard regarding what went well. The new Fellows Smart and Dawson will receive their plaque later at *Eurocrypt*, whereas Shoup and Halevi opted for *Crypto'16*.

Action Point **7: Cachin** *(Crypto'16)*:
Write guidance on the staging for the Fellows Committee to ensure a smooth handover.

4.3. **Audit Committee.** Rose has spoken to Berson and the audit committee will have a more thorough discussion in June.

Action Point **8: Rose, Audit Committee** *(June)*:
Commence an audit in time for (preliminary) reporting at *Crypto'16*

4.4. **Election Committee.** This year there will be four officers and three directors up for election.

Decision 3. *Abdalla, Abe, and Smart are appointed to the Election Committee 2016.*

4.5. **Ethics Committee.** The Ethics Committee has been receiving a number of cases. These are discussed in confidence. One emerging trend is that program chairs might need more protection from authors of rejected submissions.

Action Point **9: Ethics committee** *(no time set)*:
See whether the PC/Ethics Guidelines need an update

The Board has a discussion on the policy of the IACR ePrint archive. The current phrasing on the website is deliberately not exhaustive with a clear mandate for the editors to reject papers. While it suffices overall, it might be possible to clarify the guidelines.

Action Point **10: Boldyreva, Smart, Preneel** *(no time set)*:
Clarify the ePrint policy guidelines.

4.6. **Schools Committee.** There is no further update from the Schools Committee.

5. Program Chair and other appointments

5.1. **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.

5.2. **Crypto'17–'18.** Jonathan Katz has already been appointed as one of the co-chairs for *Crypto'17*. Several excellent candidates are nominated, and after discussion a candidate is selected.

Decision 4. *Hovav Shacham is appointed Program Chair (rolling co-chair) for Crypto'17 and Crypto'18. [Shacham subsequently accepted.]*

5.3. **Asiacrypt'17–'18.** Tsuyoshi Takagi has already been appointed as one of the co-chairs for *Asiacrypt'17*. Several excellent candidates are nominated, and after discussion a candidate is selected.

Decision 5. *Thomas Peyrin is appointed Program Chair (rolling co-chair) for Asiacrypt'17 and Asiacrypt'18. [Peyrin subsequently accepted.]*

6. Conference Proposals

6.1. **Asiacrypt 2018.** Dawson presents a proposal to host *Asiacrypt'18* in Brisbane, Australia. The Board thanks Dawson for an excellent presentation. The Board believes it is a solid proposal; there is some feedback on the budget.

Decision 6. *Asiacrypt'18 will be held in Brisbane (Australia) and Josef Pieprzyk is appointed General Chair.*

6.2. **Eurocrypt 2018.** There are two proposals for *Eurocrypt'18*. Fischlin presents a proposal to host the conference in Darmstadt, Germany, and Dunkelman presents a proposal to host it in Tel Aviv, Israel. The Board thanks both Fischlin and Dunkelman for their excellent presentations.

It is noted that, as some scientific communities boycott Israel, attendance at Tel Aviv might be lower than in Darmstadt However, travel itself is not believed to be a serious issue. Darmstadt's budget has very high fixed costs, but is a solid proposal.

Faced with two such good proposals, the Board discusses whether to already award *Eurocrypt'19*, so both bids are successful (both Dunkelman and Fischlin had indicated a willingness to bid for 2019 if unsuccessful for 2018).

Decision 7. *Eurocrypt'18 will be held in Tel Aviv (Israel) and Orr Dunkelman is appointed General Chair.*

Moreover, subject to confirmation of dates and approval of a budget, the Board decides as follows.

Decision 8. *Eurocrypt'19 will be held in Darmstadt (Germany), Marc Fischlin is appointed General Chair, and Ahmed Sadeghi General co-Chair.*

Cachin wonders whether having a *Eurocrypt* steering committee (similar to the *Asiacrypt* one) would be useful to delegate part of the selection procedure to the Board. However, from a practical perspective (e.g. timing) this appears quite hard.

7. Procedures and Guidelines

7.1. **Discussion of needed revisions.** The guidelines have not yet incorporated recent changes in practices and regulations.

Action Point **11: Cachin,Rose,Rogaway,Stam** *(1 August)*:
Have a read through various guidelines for a general clean up and ensuring they are all current.

7.2. **Privacy policy and distributing attendee lists.** The current policy was drafted by McCurley. Although we do no want to publish these data electronically, the question is how much value the current paper lists of attendees have. Preneel mentions that for some people retrieving their e-mail addresses based on publicly available information can be hard.

Action Point **12: Cachin** *(no time set)*:
Cooperate with the Membership Secretary and Communications Secretary on how to make membership and attendee information available to members and attendees.

8. Current publications

Preneel will send an update by email.

9. Conference Strategy

The Board encourages colocated workshops and schools attached to IACR Conferences. Paar wonders whether for Steering Committees a colocation chair makes sense.

10. Event reports since last BoD Meeting

10.1. ***Crypto'15.*** Nothing to report from Ristenpart (GC *C'15*).

10.2. ***Asiacrypt'15.*** Cachin (obo Galbraith GC *AC'15*) mentions that a report is uploaded.

11. Forthcoming Conferences

11.1. ***Crypto'16.*** LaMacchia (GC *C'16*) reports that acceptances are out with roughly a 25% acceptance rate. The program agenda will look quite similar to last year with one plenary session. The budget has been updated; it appears that the registration fee will be higher than last year. CHES will be colocated: the main joint events are the Crypto Rump Session, a plenary session (invited speaker) on Wednesday morning, and the Crypto Café on Wednesday evening. LaMacchia calls for participation in a possible charity auction.

Cachin thanks LaMacchia.

11.2. ***Asiacrypt'16.*** Hieu (GC *AC'16*) reports that everything is going well, the hotel has been fixed and sponsorship is starting as well. There will be an IACR supported one-week school on the foundations of cryptology beforehand.

Cachin thanks Hieu.

11.3. ***Eurocrypt'17.*** Pointcheval (obo Abdalla GC *EC'17*) mentions that the dates have moved a few times, but they are now final (and on the website). The week before, EuroS&P will take place in Paris. There are already five sponsors. There is a brief discussion regarding the desirability to book the room for Tuesday afternoon, e.g. in conjunction with a call for workshops.

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

12.1. ***CHES* Steering Committee.** The *CHES* Steering Committee has approved a proposal for Taiwan; it will be sent to the board by email.

12.2. ***FSE* Steering Committee.** Preneel (SC *FSE*) has nothing further to report.

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

12.4. ***TCC* Steering Committee.** No further update from the *TCC* Steering Committee.

13. Closing Matters

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

- the IACR *Transactions on Symmetric Cryptology*;
- the search for a new Editor-in-Chief for the *Journal fo Cryptology*.

13.2. **Review of Action Points.** After a review of action points, Cachin closes the meeting at 18.17.

14. Intermediate Board Decisions

Decision 9 (22 July 2016)**.** *Kenneth G. Paterson is appointed Editor in Chief of the Journal of Cryptology for the period 2017–2019.*

Note that this means that the EiC Search Committee has done its job and is disbanded.