MINUTES IACR BOARD MEETING *VIRTUAL-1 '20*

11 MARCH 2020

1. Opening Matters

1.1. **Welcome, roll of attendees, identification of proxies.** At 15h02 CET Abdalla opens the meeting and briefly goes around for an introductory round, confirming attendees and establishing who is holding proxies. There are 23 full time attendees with Stebila holding proxy for Paterson. Moreover, Christina Boura (General Chair *FSE'20*) and Markulf Kohlweiss, Petros Wallden, Vassilis Zikas (General Chairs *PKC'20*) are present. Kim leaves the meeting at 16h00 CET.

1.2. **Review and approval of agenda.** 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.

1.2.1. *Roll of Attendees.*

Attendees (Elected). Michel Abdalla (President 2020-2022); Shai Halevi (Vice President 2020-2022, *TCC* Steering Committee); Brian LaMacchia (Treasurer 2020-2022); Joppe Bos (Secretary 2020-2022); Masayuki Abe (Director 2018-2020); Marc Fischlin (Director 2020-2021); Nadia Heninger (Director 2019-2021); Tancrède Lepoint (Director 2018-2020); Anna Lysyanskaya (Director 2019-2021); Bart Preneel (Director 2020-2022, *FSE* Steering Committee); Peter Schwabe (Director 2020-2022); Francois-Xavier Standaert (Director 2020-2022, *CHES* Steering Committee); Moti Yung (Director 2018-2020, *PKC* Steering Committee).

Attendees (Appointed). Foteini Baldimtsi (Communications Secretary (2019-2022)); Lejla Batina (*Eurocrypt'20* General Chair (2019-2020)); Colin Boyd (*Eurocrypt'21* General Chair (2020-2021)); Jian Guo (*Asiacrypt'21* General Chair (2020-2021)); Kwangjo Kim, (*Asiacrypt'20* General Chair (2019-2020)); Leo Reyzin (*Crypto'20* General Chair (2019-2020)); Douglas Stebila (Membership Secretary (2017-2020)); Vladimir Kolesnikov (*Crypto'21* General Chair (2020-2021)).

Attendees (Representatives and Others). Kevin S. McCurley (Database Administrator); Tal Rabin (Code-of-conduct Liaison);

Absentees (Appointed). Kenny Paterson (Journal of Cryptology Editor-in-Chief 2017–2019, *RWC* Steering Committee);

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

2. Appointments, committees and policies

2.1. **Election committee.** The President recalls that last election most elected members came from Europe. It is important to represent all our members. Abdalla asks for volunteers to join the election committee and would urges to get candidates engaged earlier than previous years: preferably before *Crypto*. Lysyanskaya and Preneel volunteer.

> Action Point **1: Abdalla** *(no time set)*:
> Form the Election Committee and include Lysyanskaya and Preneel.

2.2. **JoC Editor-in-Chief.** The President explains that the Board needs to look for a replacement of Kenny Paterson. Paterson was supposed to step down last year but agreed to a one year extension. Abdalla will form a committee to look for a replacement: Paterson indicated that he wants to be part of this committee. Lysyanskaya volunteers Reyzin for this committee but Reyzin indicated that due to the coronavirus situation around *Crypto'20* he would rather focus on this instead.

> Action Point **2: Abdalla** *(no time set)*:
> Form a committee to look for the JoC EiC replacement.

Abdalla thanks Paterson for all the work done and agreeing to the one year extension.

3. BUDGET AND FINANCIAL

3.1. **IACR Budget 2020.** The Treasurer goes over the FY20 Non-Conference Operating Budget provided in the repository. The student speaker budget is kept the same as last year. Overall, there is a small negative amount which needs to be approved.

Decision 1 (unanimous)**.** *The Board approves the FY20 Non-Conference Operating Budget.*

LaMacchia further provided an update with respect to progress on the IACR's investment strategy and implementation at Fidelity Investments. We also lost the ability to utilize TransferWise for discounted international currency conversions and transfers as TransferWise is no longer licensed to provide services to Nevada-based entities. The Treasurer sees three options: setup delegate payment processor in another state, move the legal home of IACR to another state, or hope TransferWise gets a license in Nevada again. Halevi proposes to postpone this discussion to the Board meeting at *Eurocrypt*.

Abdalla thanks LaMacchia for his great work.

4. TOPICS

4.1. **Program Chair Guidelines.** Preneel recalls the changes and history of this task. The changes to the guidelines include the change to the parallel co-chair model. However, this revision work started to take into account the hybrid models (*CHES* and *FSE*). There are *many* other minor changes made to improve the document and make it more up-to-date. This document was submitted September last year to the President. Preneel points out that all comments received have been incorporated. This should go out as soon as possible for better guidance.

There follows a discussion on the timeline for submitting the final version of the accepted paper. This focuses on the visa requirements versus the freshness of papers. Reyzin suggests to make the timeline for submitting final versions shorter. Abdalla notes that people generally only apply for a visa when their paper is accepted. Preneel suggests to change the text to two months and clearly state that Springer requires 6 weeks.

McCurley wonders why the text related to the physical PC meeting is still there. Preneel agrees and admits he was amazed about this as well. However, multiple people preferred to keep this text in. Abe asks if we can add text to make it clear to mention the top-3 papers in the foreword of the proceedings; Preneel agrees and will make this change.

Abdalla suggests to vote on these guidelines another time since more changes are needed. Preneel urges to move forward since the guidelines are currently really outdated and there are always minor changes to be made. He suggests a one week period for review, comments and modifications and then release this version. Abdalla agrees and thanks Preneel for all his work on updating the Program Chair Guidelines.

Decision 2 (unanimous)**.** *The Board approves the new Program Chair Guidelines modulo minor changes which should be received within a week from this virtual Board meeting. If significant concerns or comments are received then this vote has to be redone. If not, then the new guidelines will be put online.*

4.2. **HotCRP and ePrint.** McCurley provides an overview of the recent activities. This includes; all code and tracking moved to github. We now have tools for maintaining conference websites: *Asiacrypt'20* will be the first one to use this. Deployment of HotCRP on the servers of the IACR together with Cachin; this is currently used by *Crypto'20* and *ToSC*. The copyright forms are outdated, Preneel volunteers to update these.

> Action Point **3: Preneel** *(no time set)*:
> Update the copyright forms.

McCurley starts a discussion related to websubrev versus HotCRP and thanks to Halevi for all his work over the past years. The full Board agrees and thanks Halevi. McCurley questions why we are investigating switching to HotCRP: HotCRP codebase is poorly documented and poorly structured. Both websubrev and HotCRP only solve part of our publishing process. Halevi points out that the main advantage of websubrev is the IACR integration: this needs to be added if we switch to HotCRP. McCurley asks for the automated script which creates a new instance of websubrev.

> Action Point **4: Halevi** *(no time set)*:
> Provide the scripts which automatically create a new websubrev instance to McCurley.

Heninger recalls that we switched to HotCRP at the request of Ristenpart. She points out that HotCRP is much nicer to use for the end-user compared to websubrev.

4.3. **Eurocrypt 2020 update.** It is agreed that this will be discussed later (see Section 4.5).

4.4. **Code-of-Conduct General Guidelines.** Rabin gives a summary of the activities and code-of-conduct issues at the recent *RWC* symposium. We need a lawyer for legal guidance; moreover, the IACR does not currently have a complaint form online. Yung recommends to explore our connections with UCSB to get in contact with good lawyers. LaMacchia agrees we need an attorney and we should prepare an engagement letter.

> Action Point **5: Rabin** *(no time set)*:
> Find a suitable lawyer and setup guidelines.

4.5. **Coronavirus impact.** The *FSE* conference has been postponed. The number of people not able to attend was significant. Moreover, no conferences are allowed in the upcoming weeks by the Greek government. We are looking for new dates with no financial impact.

The situation for *Eurocrypt* and *PKC* is similar. Batina explains that the expected number of attendees would be significantly lower. Croatia is already closing public schools and the situation is getting worse. The current plan is to postpone *Eurocrypt* without additional cost to the fall. Halevi agrees we need to postpone or decide to do a virtual conference: make this decision as soon as possible. The President agrees and emphasizes the safety of our community.

Wallden explains that the current peak is expected in two months and postponing *PKC* is preferred. At the moment they received only very few registrations (three in total). LaMacchia observes that it is not a good idea to put everything in the fall since this will overwhelm the community. Halevi urges to take the participants points of view into account; is it desired to have many conferences in the same month(s)? Batina points out that canceling a conference has a significant cost while postponing does not.

Heninger suggests to give authors the option to present at special sessions at other IACR venues. Stebila likes this flexible suggestion since publication will happen anyway.

The President concludes that hosting events in May is impossible. Postponing *Eurocrypt* seems the safest option. Standaert asks if postponing by one year is a possible solution. Batina explains that this was not discussed with the venue but it might be possible. What about *Eurocrypt* in Norway? Boyd explains this should be possible even if the contract is signed.

The President does not want too many events in the fall. Maybe combine this with *Crypto* or allow virtual presentations. Since no physical Board meetings are expected he will plan more frequent virtual Board meetings.

Decision 3 (unanimous)**.** *The Board decides that the President has full authority to make quick decisions regarding postponing and canceling IACR events. This will be done in close contact with the Treasurer, General Chair(s) and relevant Steering Committee of the affected events.*

5. Closing Matters

Abdalla closes the meeting at 17h15 CET.