MINUTES IACR BOARD MEETING *VIRTUAL-8 '21*

12 AUGUST 2021

1. Opening Matters

1.1. **Welcome, roll of attendees, identification of proxies.** At 16h00 CEST Abdalla opens the meeting and briefly goes around for an introductory round, confirming attendees and establishing who is holding proxies. There are 20 full time attendees with Halevi holding Lepoint's proxy, Stebila holding proxies for Bos and Fischlin, Lysyanskaya holding Baldimtsi's proxy, Batina holding Schwabe's proxy, and Preneel holding Rijmen's proxy. During Halevi and Kolesnikov's absence, Bishop holds their proxies.

1.1.1. *Roll of Attendees.*

Attendees (Elected). Michel Abdalla (President 2020-2022); Shai Halevi (Vice President 2020-2022, *TCC* Steering Committee); Brian LaMacchia (Treasurer 2020-2022); Masayuki Abe (Director 2021-2023); Nadia Heninger (Director 2019-2021); Anna Lysyanskaya (Director 2019-2021); Bart Preneel (Director 2020-2022, *FSE* Steering Committee); Francois-Xavier Standaert (Director 2020-2022, *CHES* Steering Committee).

Attendees (Appointed). Lejla Batina (*Eurocrypt'20/'21* General Chair (2019-2021)); Allison Bishop (*Crypto'22* General Chair (2021-2022)); Colin Boyd (*Eurocrypt'22* General Chair); Jian Guo (*Asiacrypt'21* General Chair (2020-2021)); Vladimir Kolesnikov (*Crypto'21* General Chair (2020-2021)); Douglas Stebila (Membership Secretary (2017-2022)); Bo-Yin Yang (*Asiacrypt'22* General Chair (2021-2022)); Moti Yung (Director 2021-2023, *PKC* Steering Committee).

Attendees (Representatives and Others). Kevin S. McCurley (Database Administrator); Yu Yu (Webmaster).

Absentees (Elected). Joppe Bos (Secretary 2020-2022); Marc Fischlin (Director 2020-2021); Tancrède Lepoint (Director 2021-2023); Peter Schwabe (Director 2020-2022).

Absentees (Appointed). Foteini Baldimtsi (Communications Secretary (2019-2022)); Vincent Rijmen (Journal of Cryptology Editor-in-Chief 2021–2023).

Absentees (Representatives and Others). Hilarie Orman (Archivist); Tal Rabin (Code-of-conduct Liaison);

1.2. **Approve minutes from last BoD virtual meeting.** The President thanks the Secretary for the completion of the minutes which have been shared before the current Board Meeting. Abdalla calls for a vote to approve the minutes.

Decision 1 (unanimous)**.** *The Board approves the Minutes of the IACR Board Meeting Virtual-7 '21.*

1.3. **Update on Committees.** The President gives an update on the Elections and Fellows committees. The Elections committee will consist of Abe, Halevi, and Lepoint. Lysyanskaya and Kim will be stepping down from the Fellows committee; and it is noted that Peikert stepped down last year. Abe and Sasha Boldyreva will be joining the Fellows committee. An ad hoc committee to discuss program chair selection criteria has been struck consisting of Abe, Preneel, Yang, Yung, and Tal Rabin. LaMacchia notes that the audit committee has not met since the last meeting.

> Action Point **1: Baldimtsi** *(no time set)*:
> Update lists of committee members on website.

2. Conferences

2.1. **Crypto 2021 update.** Kolesnikov gives a report that preparations for Crypto 2021 are proceeding well. McCurley may be called away during part of the event but a backup plan is in place. Registration count is currently 648. We anticipate approximately $50-55,000 in sponsorship.

2.2. **Update on 2021 conferences.** Guo gives an update on Asiacrypt 2021. While vaccination in Singapore has proceeded quickly, cases remain high. The government currently plans to fully open by the end of September and is negotiating with neighbouring countries for a possible travel bubble, but prospect is unclear. A final decision on any physical component for Asiacrypt 2021 remains postponed until the end of the month, but at this point they are planning for a fully virtual event. Abdalla asks that the Asiacrypt steering committee decide whether they intend to shift subsequent Asiacrypt events or not; Guo is open to hosting Asiacrypt in Singapore in a subsequent year, but Abdalla notes that Guo will be program committee co-chair of Asiacrypt 2023 which should be taken into account on any shifting plans.

Abdalla reports that Eurocrypt 2021 continues to plan for a hybrid event. However, as the number of cases has increased since our last meeting, in-person attendance may be further impacted. Batina reports that planning with the hotel and a budget will be finalized in the coming weeks, currently planning for 200 in-person attendees. Potential losses should be low as there have been few commitments to date. There are currently plans for 5 workshops that would take place in-person.

McCurley gives an update on CHES 2021. CHES 2021 will as previously decided be happening fully online. Notifications for the last included issue of TCHES have just gone out, so those authors will be contacted shortly to arrange video uploads. McCurley expects everything to proceed according to plan.

Abdalla notes that no final decision has been made for TCC 2021, which is currently hoping for an in-person hybrid event. At present entry to the United States is restricted.

LaMacchia reports on RWC 2022. At present there is a hope to have some in-person component, but no decision has been made at this time. Assembly of the scientific program as well as sponsorship proceeds as normal.

3. Appointments, committees, and policies

3.1. **Crypto 2023 general chair appointment.** The President recalls the Board needs to select the General Chair for Crypto 2023. Abdalla suggests that we consider soliciting volunteers for General Chair for Crypto in future years. Several excellent candidates are nominated, and after discussion a candidate is selected.

Decision 2. *Britta Hale is appointed General Chair for Crypto 2023. [Hale subsequently accepted.]*

4. Topics

4.1. **IACR Financial Update.** LaMacchia provides a brief update on the financial status. LaMacchia continues to following investment committee policy on moving investments over to Fidelity. We have continued to receive very strong sponsorship support for our virtual events (more than $100,000 for 2021 events) yet our costs remain quite low. Some funds have been allocated for TCC 2021. LaMacchia notes we still do not have a low-cost solution for easily transferring money internationally due to our loss of access to TransferWise. McCurley notes that the strong financial position may allow us to consider using Gather.town for an event. A discussion ensues highlighting the need to remain conservative in the coming years due to potentially increased costs of hybrid events, continued risk future cancellations of in-person events, and ongoing uncertainty over attendance. Preneel suggests that we should aim to not increase registration costs despite fewer attendees as this may further depress registrations, and acknowledges that this may incur some loss.

4.2. **Sponsorship of IACR outstanding papers.** Yu presents a proposal from PlatON to sponsor outstanding papers awards at IACR conferences, resulting in a $1,000 award for each best paper / best young researcher paper / best student paper at IACR conferences over the next 10 years. Abdalla notes that there would be tax issues with regards to the IACR giving money to award winners. (In contrast, RWC's Levchin prize is paid directly from the sponsor to the awardee, rather than via the IACR.) Abdalla comments that this yields a fairly high profile sponsorship with a relatively low amount of sponsorship per event, often lower than the amount contributed by other sponsorships. Abdalla suggests that if the IACR wants to consider sponsored best paper awards, it might be better to have an open call for such proposals. LaMacchia notes that 10 years is a long period of time to bind the IACR, and notes that the Board would be imposing on the program committee the requirement to select best papers as well as centralizing a sponsorship activity. LaMacchia says that we would need to collect and distribute tax forms for winners and would need to ensure that any contract preserves IACR's independence. Yung says that an awards policy should be carefully thought out by the organization rather than driven by external funding. A straw poll of members indicates lack of support for establishing an award as per PlatON's proposal at this time.

5. Closing Matters

Abdalla closes the meeting at 17h51 CEST.