MINUTES IACR STRATEGIC MEETING AT *EUROCRYPT 2023*

23 APRIL 2023

1. Opening Matters

1.1. **Welcome, roll of attendees, identification of proxies.** At 14h18 CEST Abdalla opens the meeting and briefly goes around for an introductory round, confirming attendees and establishing who is holding proxies. There are 21 full time attendees with the following proxies: Poettering holds Hesse's proxy (when absent).

1.1.1. *Roll of Attendees.*

Attendees (Elected). Michel Abdalla (President 2023-2025); Allison Bishop (Vice President 2023-2025); Brian LaMacchia (Treasurer 2023-2025); Benjamin Wesolowski (Secretary 2023-2025); Masayuki Abe (Director 2021-2023); Jian Guo (online, Director 2022-2024); Shai Halevi (online, Director 2023-2025); Anna Lysyanskaya (Director 2022-2024); Bart Preneel (Director 2023-2025, *FSE* Steering Committee, Program Chair Contact); Peter Schwabe (online, Director 2023-2025); Bo-Yin Yang (Director 2022-2024); Moti Yung (Director 2021-2023, *PKC* Steering Committee);

Attendees (Appointed). Britta Hale (*Crypto 2023* General Chair (2022-2023)); Julia Hesse (*Eurocrypt 2024* General Chair (2023-2024)); Bertram Poettering (Membership Secretary 2023-2025); Damien Stehlé (*Eurocrypt 2023* General Chair (2022-2023));

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

Absentees (Elected). Tancrède Lepoint (Director 2021-2023, *Crypto 2024* General Chair (2023-2024));

Absentees (Appointed). Foteini Baldimtsi (Communications Secretary 2023-2025); Vincent Rijmen (Journal of Cryptology Editor-in-Chief 2021-2023); Bimal Roy (*Asiacrypt 2024* General Chair 2023-2024); Fangguo Zhang (*Asiacrypt 2023* General Chair (2022-2023));

Absentees (Representatives and Others). Tal Malkin (*TCC* Steering Committee); Mitsuru Matsui (*Asiacrypt* Steering Committee); Hilarie Orman (Archivist); Kenny Paterson (*RWC* Steering Committee); Tal Rabin (Code-of-Conduct Liaison); Yu Yu (Webmaster);

2. Co-location of conferences

The President recalls the proposition of co-locating conferences: a flagship conference and an area conference could be held at the same place as a way to reduce the environmental impact of travel. This has already been tried with *Crypto* and *CHES* (in 2010, 2013, and 2016), but this was not a conclusive experiment and *Crypto* and *CHES* attract different people. The President adds that *CHES* and *RWC* are both hard to merge with the rest of the community — it would be easier with *TCC*, *FSE* and *PKC*.

Preneel notes that this discussion should be coordinated with the steering committees of area conferences. Although a good idea to reduce travel, it may face some resistance from the community.

Co-location could simply mean that the events happen in *nearby* cities, not necessarily in the same venue or city. Schwabe adds that holding both in the same venue could be problematic. Bishop says that by holding the events in the same city (but different location), the general chairs may share some of the work. Yung says we would need to choose the venue for the flagship conference first (as this is generally harder, due to the larger scale of the event), and the area conference would have to work with it. This process may be hard to optimise.

Guo notes that some flexibility is needed in which area conference is associated to which flagship. For instance, *FSE* often takes place around spring, hence could naturally be paired with Eurocrypt — but *FSE* should not always happen in Europe.

It is suggested that the transition be gradual, first encouraging experimentation.

> Action Point **1:** *(no time set)*:
> Approach the steering committees of the area conferences. Ask them to consult with their communities about the matter: how to best implement co-location of events?

Yung points out that we should not forget about areas of the world that do not have a flagship conference (like Africa).

Lysyanskaya adds that co-location with relevant non-IACR conferences may be an option: *CT-RSA*, *ACM CCS*... Coordination with other organisations would be required. Someone on the board could be designated as liaison.

3. Policies on remote/hybrid conferences and presentations

Abe starts by commenting on the case of *PKC*: the call for paper states that "authors of accepted papers must guarantee that their paper will be presented at the conference". If authors do not want to come, is that fine? During the COVID-19 period, this sentence was interpreted in a relaxed sense, with remote presentations. Stehlé comments on the case of *Eurocrypt*: to maximize in-person talks, authors who could not come could designate a proxy speaker.

A discussion ensues on the advantages and issues of authorizing remote presentations. Remote presentations degrade experience for in-person attendees. Some employers may not let their employees travel to present their results if remote is an option. Some employers do not want their presentations streamed or recorded (that happened at *RWC*, and maybe there should be a policy against that?).

Possible solutions are then discussed. Presently, exceptional situations (like visa issues) are accommodated, but it is expected that authors who do not want to travel somewhere should not submit to that conference. It is mentioned that decoupling publication and conferences may be a good idea. It is possible to ask (at submission), whether an author wants to present the paper (that should not affect the chances of being accepted), and only these papers would be allocated a slot in the conference program. If most papers are presented, that change would not have a big impact on the conferences; and if many papers are not presented, maybe that would lighten the program and solve the double/triple track issue. Some concerns are raised: would the conferences remain attractive?

Stehlé mentions another option: occasionally having fully online conferences. They would have the same scope as the flagship conferences, but would be a welcoming venue for the many people who cannot travel.

No consensus is reached, and this discussion is to be continued. The general opinion seems to be that remote talks at in-person events are deprecated, but coupling publication and travel is an issue to be solved.

4. Double vs. triple tracks

The president introduces the next point on the agenda, addressing the increasing number of submissions and the transition from double track to triple track for the flagship conferences, as is already implemented at *Eurocrypt 2023*.

Yung expresses concern about the potential negative impact of sticking to fewer tracks: it would result in being more selective and ultimately lead to fewer publications. This, in turn, could be detrimental to the careers of cryptographers. LaMacchia responds that publication and presentation slots should not be conflated. The importance of maintaining the acceptance rate is emphasised; it is noted it could even be increased as long as there are enough high-quality papers.

The President points out various implications of increasing the number of tracks, including the need for more expensive venues (hence higher registration fees), increased workload for organizers (hence the potential requirement for assistance from professional organizers). Triple tracks essentially disqualify academic venues, resulting in higher prices and limited catering choices.

A suggestion is made to replace 20-minute talks with 5-minute pitch talks, which sparks a discussion. 5-minute pitch talks would not be compatible with requiring in-person presentations. Bishop notes that talks are seen by students as the least valuable aspect of a conference.

Other ways to scale should be considered, such as poster sessions. McCurley mentions that the machine learning community has transitioned to poster sessions. Hale expresses concern that poster venues may negatively impact students' careers, as they may not be valued equally by every institution. A discussion ensues, clarifying that the conference would not be entirely poster-based. All accepted papers would still be included in the proceedings, with some having a presentation slot and others assigned to poster presentations.

The Treasurer provides information on the financial impact of implementing triple tracks, citing an increase of approximately 250 USD per participant based on early estimates for *Eurocrypt 2023* in Zurich. After adjustments, the difference was reduced, but triple tracking would still result in a registration fee of around 1000 USD per participant. A quick poll among the board members indicates that the 1000 USD registration fee is an alarming increase.

A temporary conclusion was reached to stick with triple tracks for the time being, while closely monitoring the budget and investigating long-term solutions. The Treasurer emphasized the need to have sufficient funds in the treasury to handle a complete loss of an event, such as in the case of a pandemic (hence increasing the budget of our events has an impact on that front).

5. Publication model for flagship conferences

The President introduces the next point on the agenda: the publication model. Currently, Springer publishes the proceedings of the flagship conferences. The question arises whether we should change that model, and whether we should move to self-publishing.

McCurley confirms that self-publishing is viable. Area conferences have already successful experimented with self-publishing, and there are ongoing efforts to decrease the human time spent on each paper. Preneel points out that Springer handles certain tasks such as fixing references, white spaces, and ensuring LaTeX files compile. These are tasks that we could handle ourselves. McCurley emphasizes the need to comply with the constraints of commercial indexing references like Scopus (for example, collecting authors' countries).

The merits of self-publishing were compared to staying with Springer for the general conferences and the area conferences *PKC* and *TCC*. In the past years Springer encountered issues, such as the proceedings not being available at the time of the event.

McCurley briefly describes an alternative publication model described in the document *A Proposal for Re-organizing the IACR Publications Landscape*, by Gaetan Leurent. This model is referred to as Proposal 8, and essentially suggests to create a single journal for the flagship conferences. It would replace the proceedings of *Crypto*, *Eurocrypt* and *Asiacrypt*. Authors would submit to the journal, and some rule would determine in which conference they present. Proposal 8 may be compatible both with staying with Springer, or with moving to self-publishing.

The Secretary asks if anyone sees any downsides to Proposal 8. Most attendees express a favorable opinion of the proposal. The only potential downside mentioned is that it would change the current writing and reviewing practices, notably changing how we currently deal with appendices (currently excluded from proceedings).

6. Revise and Submit experiment

Lysyanskaya introduces the last point on the agenda: the Revise and Submit experiment between Eurocrypt and Crypto. She explains that papers that were almost accepted at Crypto but didn't make it were invited to resubmit to Eurocrypt, with one of the original reviewers joining the next reviewing team. A total of nine papers were invited, out of which five successfully followed the instructions, two attempted but failed, and two declined. There were a total of 75 resubmissions.

Lysyanskaya notes that although the sample size is small, they observed a higher acceptance rate compared to "simple" resubmissions. This outcome is not surprising since the invitees were already close to being accepted. Halevi suggests continuing the experiment until they gather sufficient feedback from the participants.

Hesse raises the point that this approach requires a higher commitment from the reviewers, as they are asked to join a committee and would be needed again a few months later. Preneel responds that this is already the situation with journals, where reviewers follow revisions, and it has proven to work well.

It is highlighted that carrying the token from one conference to the next is the responsibility of the authors. The idea of a journal/conference hybrid (such as Proposal 8) would make the process more automatic and fluid.

7. Closing Matters

Abdalla closes the meeting officially at 18h10 CEST.