

# MINUTES IACR STRATEGIC MEETING AT CRYPTO 2023

19 AUGUST 2023

## 1. OPENING MATTERS

**1.1. Welcome, roll of attendees, identification of proxies.** At 11:10 PST the Vice President opens the meeting and briefly goes around for an introductory round. There are 21 full time attendees.

### 1.1.1. Roll of Attendees.

*Attendees* (Elected). Allison Bishop (Vice President 2023-2025); Brian LaMacchia (Treasurer 2023-2025); Benjamin Wesolowski (Secretary 2023-2025); Masayuki Abe (Director 2021-2023); Shai Halevi (Director 2023-2025); Tancrede Lepoint (Director 2021-2023, *Crypto 2024* General Chair (2023-2024)); Anna Lysyanskaya (Director 2022-2024); Bart Preneel (Director 2023-2025, *FSE* Steering Committee, Program Chair Contact); Peter Schwabe (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)); Bertram Poettering (Membership Secretary 2023-2025);

*Attendees* (Representatives and Others). Kevin McCurley (Database Administrator); Hilarie Orman (Archivist); Tal Rabin (Code-of-Conduct Liaison);

*Absentees* (Elected). Michel Abdalla (President 2023-2025); Jian Guo (Director 2022-2024);

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

*Absentees* (Representatives and Others). Yu Yu (Webmaster);

The Vice President rapidly goes through the agenda.

## 2. CONFERENCES AND PUBLISHING MODELS

**2.1. Decoupling papers and talks.** Schwabe, LaMacchia and Yang have drafted a proposal *Posters by default: a proposal for IACR conferences*, sent to the Board ahead of the meeting.

LaMacchia starts by presenting the problem: our general conferences have an evident scaling issue. The growing number of publications (hence, talks) imposes constraints that become harder to satisfy at a reasonable price. We want to maintain the acceptance rate, but with the current talk format, that now requires to open a third track in the conferences' agenda. That third track is reported to cost an extra \$75K for Eurocrypt and \$120K for Crypto this year. Convention centers with enough large rooms come at a high cost. We are not the only association facing this situation (Usenix, with six tracks, has reached a registration fee of \$1200).

Should we rethink the correlation between accepted papers and presentation slots? Is the primary purpose of the conference to present papers or to bring people together?

LaMacchia adds a practical point: we are signing contracts up to three years out, so any changes must be planned well in advance.

The choice seems to be between eventually reaching 4 or 5 tracks, or moving to an alternative model, possibly replacing talks with posters. Should we decouple accepted papers from presentation slots?

It is proposed to implement poster sessions as follows. All accepted papers would still get fully published in the proceedings, and would materialize as a poster at the conference (and possibly a pre-recorded talk). Then, only a select few get a presentation slot (distinguished papers).

Opinions and ideas are collected as we go around the table.

- An opt-out option for people who don't want to present?
- The new journal may alleviate some of those growing issues.
- There are problems with poster sessions: looked down upon by universities, not the same experience.

- Having more conferences instead? or parallel venues? consecutive weeks? (counterpoints: we are already stretched thin on organisation, and it dilutes the community).

The Board is mostly in agreement that a change of model seems inevitable, but we are split on what to do. We may want to ask the community, and survey what they want to preserve about conferences.

**Action Point 1:**

Prepare questions to ask at the membership meeting on how to best handle the scaling issue of general conferences.

**2.2. Lessons learned from the new journal for other IACR publications.** McCurley has been working on the new journal for a year, particularly on the submission and copyediting processes. As a reminder: the new journal has a conference-style reviewing system, with no limit on the number of papers and number of pages. The process is as follows:

- (1) Submission on HotCRP.
- (2) Review by editorial committee.
- (3) Upon acceptance, upload of a new version, raw  $\LaTeX$ .
- (4) Compilation in the Cloud, and extract metadata from the  $\LaTeX$ , for easy reporting to indexing.

The cost should be below \$5 per paper, excluding copyediting.

Copyediting will start as volunteer effort. There will be a user interface to interact with authors and let them fix issues. Down the road, LLMs may help with copyediting.

Where does that leave us for the conferences? We could move the general conferences to a journal model. A switch may be possible in two years, hinging on how it goes for the new journal. We should be able to handle 5000 submissions per year.

Bishop initiates a brief discussion on the advantages and drawbacks of staying with Springer, now that leaving seems feasible.

**Action Point 2:**

Investigate the community's opinion on dropping Springer, and further investigate the consequences.

### 3. ETHICS AND DIVERSITY PROPOSALS

**3.1. Code-of-Conduct liaison.** Tal Rabin (Code-of-Conduct Liaison) joins the meeting to discuss two points with the Board.

- First, there is a need for more volunteers to serve as contact points for code-of-conduct issues (essentially, harassment). Particularly younger people, who are sometimes easier to approach (say, for sexual harassment issues). Adding two more senior people to the group would also be helpful, as some problems can involve influential individuals.
- Second, Rabin asks the Board about reporting. All kinds of problems happen at large conferences. To what extent does the Board need and can (legally) be made aware of any of it?

A discussion ensues about what kind of reporting can be made. It is suggested to report to the Board yearly statistics, with no specifics (even anonymized, such data could lead to legal and ethical problems). We may need legal counsel; maybe consult with the ACM ethics committee.

It is pointed out that the IACR bylaws entrust the Board with disciplinary matters; in such cases, the Board would need to know the specifics of a situation. This could be amended to delegate that power. We need to formalize the process better.

Finally, the Board discusses communication with the membership. What kind of statistics can be communicated during membership meetings? Should we survey the community about related issues (do you feel safe, supported, etc...)?

**Action Point 3:**

Add request for volunteers to the membership meeting slides.

**3.2. Action items regarding the diversity proposal.** The agenda included an item to discuss potential action arising from the diversity proposal submitted a few weeks ago. It is decided to defer that discussion to the September Board meeting.

### 4. STAFFING — INCREASING CAPACITY AND RESILIENCE

Currently, McCurley works 30 to 40 hours a week for the IACR. The work includes large-scale software projects (iacr.org, conference web templates, ePrint, HotCRP, virtual conference platform, new journal infrastructure). and a variety of routine tasks (managing the YouTube channel, uploading slides...).

How long can the IACR sustain its operations with volunteer work alone? Should we hire help?

It is noted that even if we hire help, we still need someone to manage and ensure continuity (a paid person will also not stay forever). To help with continuity, documentation of existing infrastructure should be high in the priorities.

LaMacchia notes that hiring assistance is a viable option. The IACR has savings. Sponsorship brings in money. Also, the membership fees have remained low over the years, and increasing them slightly is possible.

**Action Point 4:**

Set the scope of the work to be delegated. Clarify how to ensure continuity.

**5. CLOSING MATTERS**

The Vice President closes the meeting officially at 14:35 PST.