On Creating a More Inclusive and Supporting Community

Elena Pagnin[1], Sofía Celi[2], and Akira Takahashi[3]

[1] *Chalmers University, Sweden,* elenap@chalmers.se
[2] *Brave, Portugal,* cherenkov@riseup.net
[3] *The University of Edinburgh, UK,* takahashi.akira.58s@gmail.com

June 9, 2023

Abstract

Inspired by the panel on allyship and inclusion at CRYPTO '22, we present a call to action and some suggestions for improving the state of the International Association for Cryptologic Research (IACR) community from various perspectives. The objective of this document is to draw attention to some issues, especially those of DEI-kind (Diversity, Equity and Inclusion), along with proposed pathways to solutions that are informed by the authors' lived experiences. We hope that this document will contribute to the ongoing discourse on DEI in the IACR community, and that our proposals might spark concrete action towards creating a more equitable and diverse research environment.

We do not expect the IACR to act on all ideas, as not all fit it within its role; but we hope that this document serves as an inspiration and incentive to IACR members and individuals to offer help and take actions to improve the current state of affairs.

The IACR today represents a thriving research community, building a rich mathematical theory and applying it to serve the security needs of billions of people around the world. While initially classified as a military technology that warranted close government guardianship, cryptographic research today is produced by a community that prides itself on its open nature; indeed most publications are freely available online, and much of the research is the outcome of international collaborations. However, the mode in which the research itself is conducted is plagued by systemic issues that hamper equitable and diverese participation by all members of society. Many of these issues stem from historical inequities embedded in the broader international society, for instance discriminatory visa policies rooted in the racist legacies of colonialism translate to difficulties in conference participation tied to ethnicity and national origin. Conversations around such systemic issues are already underway in other communities[1], and it is imperative that the IACR acknowledge them and take active steps to make cryptographic research more equitable and diverse.

In this document, we put forth proposals that we believe will help the IACR foster a more inclusive and supportive community: some of the proposals are of the domain of individual program chairs, while others are of the broader organization. We do not claim to be DEI experts, and our ideas are informed by our lived experiences. While we acknowledge that in order to tackle systemic inequities one may need to work beyond the borders of the IACR, we believe that a discussion on these matters is urgently needed within the community and we propose steps and ideas that can improve the current state of affairs.

We organize our ideas into three categories: (1) Simpler tasks, (2) A bit more work—but very important, and (3) Long term goals. In addition, we organize each set of suggestion into a numbered list, for easy reference. We have outlined specific tasks that we, the authors of this document, are willing to contribute to with concrete help (ideas with actions marked with a ☆ symbol).

[1] https://www.bmj.com/content/380/bmj.p78

1 Simpler tasks

Idea 1 [Topic: **Visa support**]
Action: Create an automated template for generating visa letters for early-visa access (could be up and running after the paper submission is closed - even before acceptance outcome). ☆
Reason: Visa processing times can be arbitrarily long (specially, after the COVID-19 ongoing pandemic), and every step towards making the process smoother might help.

Idea 2 [Topic: **Online Audience Experience**]
Action: Improve the quality and effectiveness of online participation at conferences. Create online break out sessions and mingling opportunities, take inspiration from successful examples we saw during the pandemic. One good example of this happening was at CRYPTO2020, which provide a big set of online activities: Scavenger Hunt, Pseudorandom Social Mixer, and more. ☆
Reason: During the pandemic, several conferences strived to create rich experiences for online participants. However, since participation has shifted to primarily in-person more recently, online participants have been relegated to a second-class experience. This shift in priorities is unfair for a lot of participants who face barriers to physical in-person attendance. Having good quality online events will also facilitate attendance and inclusion of people located in remote areas, or with limited financial resources.

Idea 3 [Topic: **Financial Accessibility**]
Action: Offer free online participation, fee wavers (and possibly travel grants) for people located in Global South countries.
Reason: The $25 IACR registration fee alone is a non-trivial sum in the Global South, for instance corresponding to a month's worth of food in certain Latin American countries. Waiving such fees for online participants from Global South countries (and publicly advertising that such waivers are available) will remove a barrier for their participation. This seems to be part of the domain of general chairs of conferences and will need careful coordination with them. Several companies/organizations that provide sponsoring to IACR events sometimes have specific sponsoring solely dedicated to provide diversity support, or some funds are available solely for this: Internet Governance Forum, European Union or digital rights funds.

Idea 4 [Topic: **Providing Reviewer Guidelines**]
Action: Improve IACR Guidelines for Reviewers to provide more detailed instructions as well as examples of good and bad review practices. Some points of inspirations can be: peer-review process for theoretical computer science conferences and writing reviews and use terminology consistently, how not to write a review. ☆
Reason: Giving good and constructive reviews of papers/submissions is important for our community to grow. However, there are scarce guidelines on what constitutes a good review in the area of cryptology.

Idea 5 [Topic: **Social Networking in Support of Diversity and Inclusion**]
Action: Having more persistent social events in association with larger IACR events, where people from minorities are especially welcome to join (e.g., QUEER-Crypt at Eurocrypt22). ☆
Reason: At the moment these events are sporadic and relying on personal efforts to organize and advertise. A more structured network will boost communication and foster a warmer, more welcoming and open-minded environment.

Idea 6 [Topic: **Provide with Panels on Allyship and Inclusion**]
Action: In order to get the messages of diversity and inclusion and how to help (how to be an ally), we need pannels of people that are experts or working on that. For this, we can provide with similar events to what was held at CRYPTO2022. ☆

Reason: We can help with the creation of such events once a year.

2 A bit more work, but very important

Idea 7 [Topic: **Diversity Committee**]
Action: Create a diversity committee for giving policy and advice, like what exists at https://www.acm.org/diversity-inclusion, of people that are experts on those topics rather than people with a computer-science/mathematics background.
Reason: Without one, there is no clear way to report issues, and make sure that certain topics are kept in mind when organizing IACR events.

Idea 8 [Topic: **Systematization of Knowledge (SoK)**]
Action: Promote SoK papers tracks at good venues, preferrably with a suggestion for relevant topics
Reason: Without SoKs it is very hard to enter a new field. Good SoKs require competence and may contribute to the community ecosystem as much as 'yet another' proof technique. This seems to be part of the domain of general chairs of conferences, but can be encouraged as a general policy from IACR.

Idea 9 [Topic: **Ranking**]
Action: Publish an IACR-endorsed ranking system for venues with focus on cryptographic contributions ☆
Reason: Many people refer to the Australian CORE rankings to judge quality of events in cryptography. Is this really the best way? This tool could be used by the community to try to propose new metrics at home universities.

Idea 10 [Topic: **Mentorship Programs**]
Action: Find a way to assign mentor-mentee relationships, or even collect a pool of good Samaritans willing to answer questions and guide newcomers to the community. This can be done by creating an online community where cryptographers participate (of which we have many already) and were people can interact with each other. We are happy to create such a community; but, in order to be successful, it will need advertising from IACR. ☆
Reason: Reducing the damage of leaky-pipes and of certain people in mailing lists/tweeter.

Idea 11 [Topic: **Providing "Technical Writing" Mentorship Programs**]
Action: When writing a paper or a proposal, it is important to write it in a concreate, structured and clear manner. Some papers are rejected from conferences/programs not because of the quality of the idea but rather due to the writing. ☆
Reason: We can provide mentorship programs for this as well.

Idea 12 [Topic: **Shepherding**]
Action: Encourage shepherding of submissions with potential where the quality of the exposition is below the bar, but the research is sound. For minor fixes, a simple line in the acknowledgements may suffice to recognize the shepherd's contribution. For major fixes, co-authorship can be offered in exchange for guidance in improving the paper for submission to the next deadline, which could also streamline the review process.
Reason: Reviewers often reject papers just because they foresee an energy-draining rushed shepherding. Having the option to work with the authors for longer time and offering the shepherd a place among the authors may considerably boost learning experience from people who do not have the privilege of having access to eminent/knowledgeable people in the field. This can further help to include

communities of authors that may have good ideas but need help writing them down. Another idea is to have same reviewers to supervise revisions of a paper.

3 Long Term Goals

Idea 13 [Topic: **More Languages**]
Action: Translate cryptography books (simple ones) to other languages.
Reason: In some cases there is an initial barrier when it comes to language. Also creating a clear link to English terms, to facilitate googling. This task can be automated. ☆

Idea 14 [Topic: **Approaching New Topics**]
Action: Build one place that collects (links to) good learning resources to bootstrap new reach a topics.
Reason: There are several tools / lecture notes available in the web, but a structured page would be very useful for Masters, PhD students and also advisors (as a standard reference for finding trivial answers). This could eventually build a good knowledge place, that could be effectively exploited by the whole community if it also provides latex sources and snippets for common definitions.

Idea 15 [Topic: **Burnout**]
Action: Collecting (anonymous?) stories and numbers, and especially successful stories on how people came back (from a burnout experience)!
Reason: Many people suffer from it, but very few share. We need visibility on this.

Idea 16 [Topic: **Impostor Syndrome**]
Action: Collecting stories and strategies how to combat it!
Reason: Many people suffer from it, but very few share, and often the topic is avoid due to overly-confident people talk on and on.

Idea 17 [Topic: **Discrimination Stories & Allyship Guidelines**]
Action: Collecting stories of discrimination and analyse what happened and why. Create guidelines that allays could follow to leverage their privilege and help people who are in less advantage, or and tools how to step on and take the defence of discriminated people, should one witness a discrimination case in real life.
Reason: Things happen, but are rarely shared, and not many people are aware they are not alone, or that even if it has not happened to them specifically, they can be the person that makes a difference for someone else