

Decrypting Diversity Summit 2025

Report

May 8, 2026





Fig. 1: Group photo with online and in-person participants, taken & edited by David Haas.

Steering Team

Diego Aranha, Associate professor at Aarhus University [[Website](#)]

Katharina Boudgoust, CNRS researcher in Montpellier [[Website](#)]

Sofia Celi, Senior researcher at Brave [[Website](#)]

Maria Corte-Real Santos, Postdoc at ENS Lyon [[Website](#)]

Erin Hales, Researcher at Optalysys [[Website](#)]

Nora Khayata, PhD student at TU Darmstadt [[Website](#)]

Mahshid Riahinia, Postdoc at ENS [[Website](#)]

Leah Namisa Rosenbloom, Postdoc at Northeastern University [[Website](#)]

Local Team

Lucas Ottow, PhD student at LIRMM in Montpellier [[Website](#)]

Laz Panard, PhD student at LIRMM in Montpellier [[Website](#)]

Sara Sahraee, PhD student at LIRMM in Montpellier [[Website](#)]

1 Foreword

The cryptography community is rapidly expanding in both academia and industry. While producing fascinating results and having a real impact on private communication and secure computations in this world, our community still has unrealized potential to be more diverse. Diversity is crucial for the vitality and effectiveness of any ecosystem, offering varied perspectives and fostering outcomes that resonate with a broader audience.

One of the most noticeable gaps in our community is the underrepresentation of women. However, our vision for inclusivity extends beyond gender to encompass diversity in sexual orientation, race, ethnicity, national origin, health status, and disability. Achieving true inclusivity requires intentional and sustained efforts, which is why we founded the Women in Cryptography (WinC) community in 2022. Since its inception, WinC has organized a range of initiatives, including scientific seminars, virtual coffee breaks, and workshops discussing diversity. These efforts have received overwhelmingly positive feedback, leading to substantial growth over the past years.

As we look toward the future, we recognize the need for a long-term vision and an expanded platform to scale our efforts. With our event, the Decrypting Diversity Summit 2025 (DDS'25), we wanted to provide a dedicated space for the cryptography community to develop actionable strategies and long-term plans to foster a more inclusive and diverse environment. We aimed at strengthening community connections and facilitate scientific collaborations in the future. The summit served as a hub for collaboration, mentorship and knowledge exchange.

Among our activities were scientific presentations from renowned women cryptographers, poster sessions on a wide range of topics, two panel discussions, working groups on specific questions, as well as an educational talk and a workshop on the impostor syndrome.

This event was the first of its kind and we organized it from scratch. It was a huge effort, requiring the energy and time from the different organization teams throughout half a year. Given the overall extremely positive feedback from the participants, we are proud to think of the DDS as a success and hopefully being the first edition of a long sequence of future events of its kind.

We decided to write this report to provide a documentation of the DDS'25. Its purpose is twofold: it disseminates insights we reached throughout the workshop, and serves as a baseline for future events.

Table of Contents

1	Foreword	3
2	Report of the Event	5
2.1	Scientific Talks	5
2.2	Poster Sessions	6
2.3	Panel Discussions	6
	Panel 1 - Advocating for Diversity	6
	Panel 2 - Breaking the Cycle	10
2.4	Educational Talk	15
2.5	Educational Workshop	16
2.6	Working Groups	17
	Working Group 1: Community Building (Online)	17
	Working Group 2: Inclusion Beyond Borders (In-Person)	19
	Working Group 3: Disabled Cryptographers (In-Person)	21
2.7	Free Time	22
3	Participation & Financial Report	23
3.1	Participation	23
3.2	Budget	24
3.3	Costs	24

2 Report of the Event

We now report on the different events organized during the DDS'25. After describing them, we give positive remarks as well as suggestions for improvement.

2.1 Scientific Talks

Overall, we hosted two great scientific talks, both on the topic of succinct proofs, covering theoretical and practical aspects. Both speakers integrated personal anecdotes to their presentation, making them inspiring and relatable.

Our first invited talk was given by [Marta Bellés Muñoz](#), researcher at Dusk Network and Teaching Assistant at Pompeu Fabra University in Spain. Marta studied mathematics at the Autonomous University of Barcelona and later pursued a master's degree in Mathematics at Aarhus University. During those years, she combined her academic work with a career in classical music. In 2018, she returned to Barcelona and joined a project developing a blockchain-based identity system. Shortly after entering the blockchain space, she began her PhD at Pompeu Fabra University, where she focused on the use of elliptic curves in zero-knowledge proof systems. Today, she continues to teach at Pompeu Fabra University while working for a Dutch blockchain company called Dusk.

The seconded presentation was held by [Chaya Ganesh](#), Assistant Professor in the Department of Computer Science and Automation at Indian Institute of Science (IISc) in India. Before joining IISc, she was a post-doctoral researcher in Aarhus University, and prior to that she received her PhD from NYU's Courant Institute of Mathematical Sciences. Her research interests are broadly in Cryptography and Security. More recently, she is exploring efficient zero-knowledge proofs and rational cryptography. She has won the IBM global university award, Google and Protocol labs research grants, Infosys Young investigator award and Intel Rising Star Faculty award. She helps co-organize Bangalore Crypto day.



Fig. 2: Marta (left) and Chaya (right) presenting, taken & edited by David Haas.

Positive: We received very positive feedback on the scientific part of our program. The keynote talks were very interesting, educational and of high quality. All speakers included aspects related to their personal backgrounds in their presentations. We heard about multiple collaborative projects that were launched during the summit.

To be improved: The main issue we encountered with the scientific talks was that renowned women researchers are particularly busy and few were available to speak at our event.

2.2 Poster Sessions

An important objective of the summit was to actively integrate as many participants as possible in the program. Therefore, we launched a call for poster submissions, both on scientific contributions as well as community efforts. In total, we selected 11 posters, covering a large spectrum of topics, from concrete scientific results in the realm of cryptography and security to community efforts regarding minority groups.

In the hope of making the event enjoyable for online participants, we put big efforts into allowing both online and in-person attendees to see and discuss all accepted posters. To this end, we organized a separate in-person poster session and an online poster session on the gathertown platform.

Positive: Overall, we received very positive feedback on the poster sessions, especially on the online setup on gathertown.

To be improved: Many poster submissions were initiated through directly reaching out to the people involved in interesting community efforts. A list of existing community efforts could make it easier to reach out to the people. Moreover, we could improve the technical setup to present a poster to in-person attendees for online speakers.

2.3 Panel Discussions

Panel 1 - Advocating for Diversity Our panel moderator, **Nora Khayata** (PhD student at TU Darmstadt), welcomes everyone in the room and online and sets the framework of the following hour of discussions: None of us is expert on diversity, but we want to acknowledge and celebrate our diverse community and share our personal experiences with each other in the hope to make a change. Questions can be asked and voted for through the online tool Mentimeter, and the panel participants are of course free to decline replying to a question. After this, Nora starts by presenting the participants of our first panel of the summit.

Chris Brzuska (Faculty member of Aalto University), joining the panel online, is interested in cryptography, where he particularly enjoys showing that something is impossible. He also works on real-world key exchange protocols, leveraging modular techniques and formal verification. Chris advocates on behalf of the **QueerCrypt community** as a trans person.

Tako Boris Fouotsa (Postdoc at EPFL Lausanne), present in person for the discussion, is basically interested in everything around isogenies. Boris advocates on behalf of the **Africacrypt community**. He is actively involved in creating a stronger cryptology community in Cameroon and across Africa, having initiated a master and PhD program in Cameroon.

Erin Hales (Researcher at Optalysys), participating from Montpellier, is curious about post-quantum cryptography, especially fully-homomorphic encryption. Erin advocates for **Women in Cryptography (WinC)** and **people with disabilities**.

Unfortunately, **Sofia Celi** (Researcher at Brave) had to cancel her participation at the panel. She is actively involved in the **Latincrypt community** and **WinC**.



Fig. 3: Photo of the first panel, taken & edited by David Haas.

The first question Nora asks is *what are the challenges you have faced becoming a researcher because you are part of an underrepresented group?* Boris draws the picture of having to do *two* degrees at the same time: the academic degree and a life degree. The latter may involve adapting to a new country, culture, climate and/or language. He shares his experience when arriving from Cameroon in Rome for his PhD in February and being challenged by the cold. He also shares, as a non European citizen, how difficult it was during his PhD to participate at conferences as his permit of stay was never up to date. Erin joins Boris in the picture of the second life degree. As a person with disabilities, in parallel to your studies, you have to handle medical appointments, advocating for (and sadly often proving) your health situation in front of others. Besides the increased administrative overhead, a person from an underrepresented group might then want to additionally advocate for themselves and the community they are part of. This adds to the overall pile of work. Chris shares his experiences before, during and after transitioning, with a lot of confusion at the beginning. He also mentions recent challenges, like US

travel policies, while at the same time contextualizing his situation, for instance his privileges as German citizen. All panelists stress the community aspect that helped them to overcome those challenges. A supportive environment at work and outside of work is crucial to master the life degree at the same time as the academic degree.

Next, Nora asks *what the drive in academia or industry is to address diversity-related topics? What trends do the panelists observe?* Erin presents positive and negative aspects from a diversity advocate working in industry. While it might be harder to convince your industry employer that participating at diversity-related events is relevant to your work, there are often better structured worker rights, which are enforced. Especially in the UK, where employees have more rights than PhD students, who are considered students, not employees. Boris uses again the help of images to convey his message: you can see academia through good or bad glasses, depending on the research group you are part of. He stresses the importance of informing people, as members of your environment might not know your experiences. Once they know, they might be able to support you. Chris argues that more diverse environments open up the space of what is considered normal and thereby become more welcoming to everyone, not only to recognized minority groups. Nora complements with the idea (coming from Marta's talk earlier today) that diverse minds bring different perspectives.

Then she relates the first audience question: *Do you have any ideas on how to encourage people to support diversity efforts who are currently indifferent or not supportive?* Nora starts by suggesting that it is fun to be part of diversity efforts and it might help to get connected to the reality we are living in. Boris puts it into different words: understanding diversity and being empathic about other's experiences is key in an ever changing world. Chris shares the conflicting situation he finds himself in when talking about gender. While he would personally prefer not to think about gender boxes at all, he wants at the same time try to support others in understanding how gender might be impacting their lives and to support their agency in this matter. He tries to reach people through relatable situations and feelings, in order to create connections with them. Erin tries to put people's attention on the fact that everything is adapted to someone. If you do not feel the adaptation explicitly, it might just mean that it is already very well adapted to your needs.

Is there any explicit or implicit discrimination done between the qualifications from different countries by the employers? Chris explains that in his university, master studies admissions are decided in a way that the person reviewing the application is familiar with the institution from where the student is applying. Boris agrees and adds that assessing the background of a student requires the expertise of the country's specifics. And it is a reality that coming from a known and respected institute has a concrete positive impact on your path. Nora wonders whether there exist public resources that establish such rankings among institutions, as relying on the judgment of individual people might not lead to a qualified ranking. Erin

thinks that the application process should not only be inclusive with respect to the country of the applicant, but also their educational path. As a positive example, her previous university allowed students to individually prove their knowledge and skills required for master studies admission, instead of only letting people with a specific degree in.

Have you ever received a discriminatory question, how did you react and which reaction from others would you have liked to see in that situation? Before Chris gender-transitioned, a quite senior man researcher made a not-so-nice comment about him, to which a more senior women researcher reacted and intervened telling the man that this was not ok. While being a little embarrassed at that very moment, Chris was grateful to the women's reaction on hindsight. Boris admits that he received comments in the past that he decided to ignore, as sometimes he doesn't want to care about things that are not important for that moment. When receiving a comment, he also tries to understand the background of the person. Sometimes it is just a misunderstanding. And more generally, he learned to choose his battles wisely and not every battle is worth it. Erin discovered the "Sorry, what?!" reaction to be quite effective in the case of a DEI¹ offence. It gives the people the opportunity to correct or re-specify their question. She also thinks that sharing your experience with peers can help you to confirm that a situation was discriminatory. Regarding the allies, it is definitively a nice thing to advocate for the person receiving discriminatory questions. Boris also thinks that instead of criticizing someone on the spot, it can be better to talk to a person in calm afterwards.

Can you feel a pressure of representing the minority you are part of? Do you act differently because of this? Chris remembers that before gender-transitioning, he clearly felt whatever he was doing, to represent the whole group of women. Now, after the transition, even though he doesn't know any other trans man in the crypto community, he usually doesn't feel like this anymore. Erin, whenever she is the only women, she is more conscious about saying "dumb" things as it might affect the reputation of women generally. But the level of stress depends also on how diverse the environment, in which she is in, is. Boris thinks that it's good to have also occasions where people from underrepresented groups come together, while making sure that it doesn't lead to separate communities. Nora sees this as real challenge: there seem to be multiple sub communities in cryptography, but an overarching connection channel seems to be missing. Erin and Boris are optimistic that our summit will help to initiate such a connection.

Is there one piece of advice that you could give to members of your community and another piece of advice to people outside your community? Chris thinks it is important to not forget to protect and take care of yourself. For allies, he mostly wants to express gratefulness to all the friends who supported him through his gender-transition journey. Erin advises people in her community to speak and for

¹ DEI stands for Diversity, Equality and Inclusion.

allies to listen and hear, which can be distilled that both groups should be open. Boris similarly encourages his people to speak out and allies to give active support. With these empowering words, the first panel discussion is closed.

Panel 2 - Breaking the Cycle Our panel moderator, **Nora Khayata** (PhD student at TU Darmstadt), welcomes everyone and share the goals of the panel and the reason why it was organized. The panel is organized to discuss how to break the cycle of behaviors that unintentionally hinder diversity and inclusion in academia or research. Ultimately, we want to explore how to recognize and address these patterns to create a more inclusive environment. Nora adds *“in our shared space, let’s try to think about how we can improve the situation for us and our peers, be it more junior or senior.”* She mentions that we are not diversity experts, but want to share our personal experiences and hopefully make a change together. Questions to the panelists can be asked through the online tool Mentimeter. The panelists are free to decline replying. The panelists are introduced:

Ilaria Chillotti (Researcher at Desilo Inc), attending in-person, is a cryptography researcher at Desilo Inc. Before that, she worked at Microsoft research, KU Leuven, and Zama, and did her PhD at University of Paris-Saclay. Her research is mainly on FHE and she is one of the authors of TFHE which is one of the most popular FHE schemes nowadays.

Reyhane Falanji (PhD student at Linköping University), joining online, is studying computer science, looking at the formal verification of protocols. She did her master in the University of Grenoble Alpes and holds a Bachelor in computer science at Sharif University in Iran. She’s interested in sustainability, gender awareness and supporting underrepresented groups. She is a board member of the IDA PhD Council that supports and represents the PhD students of her department.

Martha Norberg Hovd (postdoctoral fellow at SimulaUiB), attending in-person, is working on fully homomorphic encryption and supervising both master’s and bachelor’s students. She completed her PhD in Cryptography at the University of Bergen, after earning her MSc in Mathematics and BSc in Physics and Comparative Literature at the Norwegian University of Science and Technology.

Adeline Roux-Langlois (Researcher at CNRS), attending in-person, has a PhD at ENS Lyon and did her postdoc at EPFL. Her research focuses on lattice-based cryptography and the theoretical hardness of assumptions such as the Learning With Errors problem. She is one of the two coordinators of the French national working group on Codes and Cryptography, where she initiated inclusion and gender-equality actions.

- *“A PhD is supposed to be hard, just deal with it.”*

Nora starts the discussion by asking a challenging question: *“One phrase that we hear pretty often is : A PhD is supposed to be hard, just deal with it. What do you think about this? How would you counter this argument?”*



Fig. 4: Photo of the second panel, taken & edited by David Haas.

Martha thinks that the statement is not correct. She thinks that although it's very important to acknowledge that doing a PhD consists of doing many things that are difficult, it is not inherently supposed to be hard; it is supposed to be supervised and tailored to the student and the student is supposed to have a network that helps them through the difficulties. She thinks there might be a sense of *survivor bias* in the statement that people, who have had a hard PhD and survived, think that everyone else should also just deal with it. Martha thinks a good approach is rather acknowledging the difficulties of a PhD, and thinking about how we can help to fix the problems.

Ilaria responds next. She thinks that people should be prepared to do a PhD and should be aware of its difficulties before starting it. She believes that contrary to school, where the goal is to pass exams, in PhD the goal is to invent new things which has more ups and downs; some days are exciting and some days are harder. But this is all normal and the students should be aware, beforehand, of this and the fact that it's okay to feel lost sometimes. This doesn't mean presenting PhD as something super hard where you struggle all the time, but rather honestly explain to the students what might happen and reassure them. Of course there should be an advisor and an environment to support you through this. Unfortunately, this is not what happens all the time.

Adeline follows. She agrees with Ilaria that one should be ready to do a PhD. She thinks that usually those with good backgrounds start a PhD and failing for them is difficult to accept. She thinks that the role of supervisors is very important to explain that failing is a part of doing research. She adds that saying PhD is 'supposed' to be hard might convey the idea that you have to work more than you are supposed to. It is very important to keep in mind that **PhD is a job** like any other job and shouldn't interfere with your personal life. Remember that you are not supposed to do more than what you'd do at any other job.

Reyhane starts. She agrees that doing a PhD can be challenging sometimes, as research is not deterministic and the relation between effort and result is not linear. The environment can play an important role, both positive and negative. She doesn't agree that one should just deal with the difficulties of a PhD alone. She rather thinks that there should exist ways for demanding what you should have; for instance, resolving conflicts with a supervisor shouldn't be done at a personal level for a PhD student. She agrees with Adeline that PhD shouldn't be more than a job and should not be the only defining factor of one's personality.

- *“Any similar misconceptions about PhD?”*

Nora continues by saying that for example, it is normalized that reviews are okay to destroy the paper without giving any positive feedback or points of improvement, and asks if the panelists have other commonly-accepted misconceptions in mind.

Martha begins. While she agrees that PhD is a job and tries to maintain this, she feels like there is some pressure to work more than the regular amount and to embody a PhD as a lifestyle. This might often come from established researchers, typically men, who have a big support system at home that allows them to be a full-time researcher, while for a lot of people, that's not the case; we don't have the capacity, nor the will, to be a researcher 24 hours a day. But there is an expectation that she feels from the outside, probably correlated to not having a permanent position. For this, she suggests putting some mental boundaries; *“I've done this and that has to be enough because I don't want to do everything that I feel is required of me to do.”*

Ilaria continues and brings up deadlines being during the weekend. She thinks that while it is usual and normalized in our community, it's unhealthy and it contributes to the idea that researchers should work over time. She thinks there should be a community effort to change it.

Adeline adds to Ilaria's point by referring to conferences that start on Sunday or Monday morning, which would require traveling during the weekend that challenges the work-life balance whether you have children or not, and suggests that this should change. She also comments on Martha's point about the expectations that comes when you look for a permanent position: recently at CNRS, when applying, you are judged based on only 5 publications, which is a good beginning to limiting judging the quality of a researcher based on how much they publish. She also thinks that it is a misconception that good researchers publish a lot. One is still a good research without working all the time.

Reyhane thinks that one of the accepted misconceptions in computer science is that the ratio of women in the community is accepted to be this low and that we cannot make a change. The mindset around this should change.

Finally Nora adds that things like changing deadlines of conferences should be among the changes that are reachable by our community. At this point, the DDS starting on Tuesday and finishing on Friday noon is appreciated by the panelists. :)

- *“How to deal with challenges, survive and thrive in this environment?”*

The question was reflected from the Mentimeter. Ilaria suggests supporting others. She says that while there’s no magical solution for problems that might occur, in any position, as future or current supervisors or event organizers, we can all support each other in some ways, e.g., by putting the deadlines in correct dates, or by telling our students not to overwork.

Adeline talks about her experience in having a small support group when she started her permanent position; it’s useful to deal with things and makes decision-making easier. She suggests that it’s very important and helpful. She also talks about counting hours as a solution to find work-life balance; she counts how much time she spends on tasks and some weeks she realizes that she’s worked too much and should get some rest.

Martha confirms Adeline’s suggestions through her experiences. She also talks about how important it is that when something happens that we feel is unfair, instead of immediately questioning our actions and judge ourselves, we should allow ourselves to be a bit more angry, and to acknowledge our feelings.

Reyhane brings up volunteer works and how they might affect our work-life balance; if you’re a part of an underrepresented group, you might get asked a lot to participate in different activities. You should feel free to say no, and the inviter should also make sure that you feel comfortable in saying no. Another possible action is to give concrete values to these works; for instance, they can count as department duties for PhD students.

- *“How do you break the cycle [for your students]?”*

Reyhane starts by mentioning that, from a PhD student’s point of view, one important thing when supervising a student or working with someone, is to make sure they know that they don’t need to work overtime and not to make a hero out of overworking. She suggests that a simple action can be to schedule your emails to be sent in work hours, even if you’re writing them out of work hours.

Martha adds that as a supervisor, you can set the expectations early on with your students to let them know that if you work late, it doesn’t mean that they need to keep up with you. Also that, especially with bachelor and master students, you should make sure they know it’s okay to have other priorities than their studies; for instance, to be open if they need to reschedule meetings due to personal reasons.

Adeline mentions that from a supervisor perspective, it’s also challenging as you can sometimes feel responsible for your students’ results and careers. It’s always important though to make it clear to them how you work, e.g., if you stay late in the evening but skip the morning, or if you’re a deadline person. You don’t want your style to affect your students in a bad way, so it’s important to communicate early on.

Ilaria follows by mentioning two things. Firstly, if you want to send late emails, you can include sentences like “please ignore this email until morning / Monday”,

which helps the reader feel not obliged to answer right away. Secondly, you can sometimes set an example for others when you're fighting against toxic behaviors. She narrates her experience that, after feeling she was overworking a lot, she started setting an alarm at 6 pm to leave her job (*"at 6:05 I'm 5 minutes late for my life."*). While at first this was not well seen by her colleagues, after a while they also realized that overworking is not life-changing and they can just get back to their life after 8 hours of work.

Nora comments by confirming that in general, it's good to be mindful in a senior position that our actions have an impact on our students. We can use this impact in a good way, for instance, to make them feel comfortable to take up space or adjust their work rhythm.

- *"How to deal with feeling left-out?"*

Nora continues by saying that specially as members of underrepresented groups, we sometimes get a lot of additional things to do such as organizing, attending conferences, being on committees, etc. So if we don't overwork, we might feel left out. How can we deal with this feeling?

Martha starts. She says that reflecting about the request or invitation helps figuring out if something is so important or valuable to us that we are okay with going the extra mile for it, or if that's not going to gain us anything so we can decline it.

Ilaria follows. She cites a phrase she finds inspiring: *"often when you say no to somebody else, you're saying yes to yourself."* She continues by saying that the rest of our lives would not just wait for us to be finished with reviews or submitting papers; we don't live to work, we work to live. We should use our time outside of working hours to take care of other things we want to do and live our lives the way we want to, instead of working all the time

Adeline adds that saying no might be challenging at first and you might feel guilty, but after a while it gets easier by realizing that it's not your responsibility and the other person can deal with receiving a no answer. She adds that another hack for feeling less overbooked can be to learn to do some tasks fast; for instance, if there's a report that you know no one reads and serves only as an administrative formality, it's okay to write it quickly and in an imperfect way. This helps gaining time doing research instead.

Reyhane concludes this part by confirming that reflection about the goals of doing some works might help with dealing with the feeling of being left out; you might have spent less time on research because you were in a hiring committee, so your paper got accepted in a less good venue that you hoped for it originally, but thanks to you being on the committee, now the hiring is a bit more fair.

- *"One final piece of advice?"*

Nora states the question which is judged not easy to answer by the panelists. She

begins herself: “at the end of the day, we’re cryptographers, we fix systems, it’s not like we’re fixing people, if we take a day off or answer a day later, no one will die.”

Adeline states her advice, aligned with what Nora just mentioned. “we’re not indispensable, but in a good way!”, she mentions that if you couldn’t work and needed some time off, still things would go fine, even things you consider important. Remembering this when you’re busy helps with allowing yourself to feel more freedom in choosing yourself over your work.

Nora thanks the speakers and the crowd leaves for lunch.

This concludes the second panel discussion.

2.4 Educational Talk

To complement the scientific program, the summit featured an insightful (online) educational talk by [Kylie Ariel Bemis](#), an assistant teaching professor at Northeastern University’s Khoury College of Computer Sciences. Kylie is a specialist in machine learning and statistical computing for bioinformatics. An enrolled member of the Zuni tribe, she is also a dedicated advocate for the Native American, LGBTQIA+, and neurodivergent communities, serving as a Rising Hearts Athlete Advocate. Beyond this, she is an accomplished writer whose fiction and poetry appear in collections such as *Nameless Woman: An Anthology of Fiction by Trans Women of Color*, *Maiden Mother Crone: Fantastical Trans Femmes*, and *Transcendent 4*.

At the summit, Kylie delivered a compelling presentation titled **Data Sovereignty under Tyranny**. The talk addressed how the rapid ascent of AI and high-tech government surveillance has introduced unprecedented challenges to the global struggle for human rights. This is increasingly visible as democratic backsliding creates environments where generative AI and the erosion of data privacy are weaponised against the public. Modern tyranny is no longer defined solely by military force; it is reinforced by the degradation of truth, the exploitation of private data, and the manipulation of information provenance.

While indigenous communities are historically and painfully familiar with such technological suppression, these tactics now pose an urgent threat to broader populations living in once-stable democracies. Kylie emphasised that by synthesizing global lessons in resistance, civil society can develop strategies to combat digital authoritarianism. She concluded that experts in digital security and data privacy play a vital, frontline role in these movements, acting as essential defenders of human rights, civil liberties, and the data sovereignty of vulnerable communities.

Positive: We enjoyed having an educational talk on the program, as it offered something different to the usual scientific talks. It complemented the discussions that the participants were having throughout the event, and therefore was interesting and well received by the audience. We hope to include more educational talks in future events.

To be improved: It is challenging to find speakers for educational talks, as they are often not in the cryptography community, so have less incentive to travel and participate in WinC events. To get around this (and for other reasons), Kylie’s talk was given online, which was a good compromise. For future events, we could also consider financial remuneration of speakers.

2.5 Educational Workshop

[Natacha Portier](#), associate professor at ENS Lyon led a workshop on *imposter syndrome*. From the abstract provided by her: “Impostor Syndrome is a widespread phenomenon: 70 percent of people have experienced feelings of *fraudulence* in their life. It is especially significant among high achieving women and academics of every gender. The syndrome is characterized by not owning your own success, thinking other people overestimate you and fearing being found out. It can be hugely detrimental to the accomplishments of one’s goal and to the well-being of the person experiencing it. The aim of this 3 hours workshop is to learn how to recognize the Impostor Syndrome in one’s thinking and to know which strategies to put into place to prevent it in order to reach your professional goals. This will be accomplished by awareness-raising through questioning and shared experiences, introducing theoretical input and giving practical implementation.”



Fig. 5: Educational talk by Natacha, taken & edited by David Haas.

The workshop was highly interactive. Natacha distributed question sheets containing background information, and participants were divided into groups of 3-4 people. One group was online. She began by defining imposter syndrome, then guided the session step by step by asking questions to recognize in which parts of

our life we feel this syndrome and why: for each question, participants submitted their responses, which were displayed anonymously on the screen. The participants could discuss within each group, followed by opportunities to raise their hands, share their perspectives, and reflect on their experiences. A few highlights of the workshop included calculating our imposter syndrome (IS) scores and learning about concepts such as the Dunning-Kruger effect. Natacha then outlined potential courses of action, both individually (e.g., knowing our triggers, writing in a journal, learning to fail, etc.) and collectively by leveraging support from those around us (e.g., asking for professional help, talking to others who face similar situations, etc.). The workshop concluded with an anonymous reflection, where participants shared their key takeaways and concrete steps they would take to address their imposter syndrome. Natacha also conducted a brief feedback session at the end of the workshop, during which several participants described the experience as very positive and highly impactful.

2.6 Working Groups

Positive: We received positive feedback on the discussion part of our program. In particular, the working groups were described as safe spaces for exchange, with a strong desire to continue the discussions after the summit.

To be improved: The main problem we encountered with the discussions was motivating online participants to actively participate.

Working Group 1: Community Building (Online)

The Importance of Interdisciplinary Spaces We began our discussion by noting the importance of hearing from and working with scholars in other disciplines on community-building and diversity efforts. Gatherings in particular inspire people to continue coming together.

Recognizing Inequitable Labor and Resource Distribution That said, we also talked about the fact that people who organize community spaces across disciplines tend to be overburdened and undervalued by their larger research communities. PhD students in particular, who have already-limited time and money, are often tasked with organizing and community care work. PhD students and members of marginalized communities are expected to generate and follow up on ideas for change. Resources for community building are limited in general, especially if the work is interdisciplinary and seen as outside funding for a particular project or specific research body. Balancing collectively-minded community building work with individually-minded “career” oriented work such as publishing papers is incredibly difficult, especially for PhD students and early-career scholars. Sourcing funding and time off to engage in organizing or even attending community-oriented workshops is a major burden

that affects all members of the community but differs among PhD students, post-docs, faculty, and industry researchers. We talked about how to make community building sustainable and avoid organizing burnout, including institutional demands for funding and valuation (see below), encouraging effort beyond participation, recruiting more people for organizing committees with rotating leadership structure (such as 10-12 people organizing, each taking the lead on some events), developing better organizational structures for distributing the work of organizing, automating processes where possible to make organizing smoother, and stepping away when needed to engage in self care, being involved in others' events but not directly organizing them.

Institutional Valuation of Community Building Work Institutions generally recognize diversity, equity, and inclusion (DEI) as important, but don't actively seek out and engage with the actual work of building DEI programs—the modus operandi is “the committee exists, we are done.” It is a bare minimum approach, far behind the amount of time and resources devoted to corporate partnerships, for example. Furthermore, it is stressful and tokenizing for members of minoritized communities in cryptography and beyond to speak on diversity issues when they are platformed for a brief session or worse, a single talk, at major conferences as part of the event, rather than as longer more structured workshop and discussion time or as an affiliated event. We discussed that one possible step towards receiving more institutional support would be to secure funding through labeling these events as teaching/departmental activities. We also discussed various mechanisms of institutional fundraising for community-building events. We asked: how do we give community building institutional legitimacy? We suggest starting with structural and cultural changes, which we discuss further below.

Establishing a Culture of Care and Curiosity Approaching conversations surrounding DEI, accessibility, and the current culture of the cryptography and computer science communities is very stressful, especially for PhD students and early-career scholars. We discussed the process of recognizing allies (for example by hearing others raise issues), the importance of raising awareness and engagement especially among senior scholars and people with power who do not attend designated spaces for discussing accessibility and DEI issues, and that it is easier to have these conversations face-to-face than it is to have them online. We asked: what might make people feel more open, safe, and welcomed to discuss these issues further? The core of the answer was in establishing a culture of care and curiosity. PhD students in particular can feel judged and overlooked. It is important for the well-being of everyone in the field to prioritize curiosity over judgment, listen rather than “label,” and acknowledge that issues exist rather than react with defensiveness. Small details like providing period products in bathrooms and checking in with participants about accessibility accommodations go a long way, but they don't often happen.

Childcare, a family rate for conference attendance, and a welcoming environment with programming and support for babies and small children would allow far greater access for parents. More existentially, we discussed the feeling of invisibility and not being seen as human, and the overall old-fashioned culture of academia. Fitting into this culture and engaging according to expectation can lead to success, and breaking in with a new perspective is very challenging. We found it ironic that the point of academia is to think critically and differently, yet the structures are so rigid. We imagine a version of “normalcy” in academia where true (rather than tokenized) diversity, equity, inclusion, and accessibility accommodation are givens, rather than exceptions to the rule.

Working Group 2: Inclusion Beyond Borders (In-Person)

Our discussion focused on several topics related to inclusion. Along the way, we raised some demands, suggested community efforts, and excitingly, the conversation sparked a new initiative we have already begun to build together.

Visa Issues To study abroad and attend meetings and conferences, people of some nationalities need visas. Visa issues exist and contain a wide range of problems (time, cost), and will have implications in different directions, for instance, scientists from certain countries don’t even submit to certain venues, and often these venues are the most prestigious ones. The visa application is not accessible online in a lot of countries, people need to travel, and some countries don’t even have an embassy of the target country, making the procedure even more difficult.

☞ **Demand 1:** The general chairs of conferences should identify countries with visa difficulties and 1) provide possibilities of restricted online participation and presentation options for affected researchers, 2) be proactive in sending invitation letters to those researchers with a proper amount of time in advance. Having letter templates beforehand would reduce the organization burden on the chair.

IACR, Conference and Renown The cryptography community is growing fast, and everyone prefers to publish in the 3 flagship IACR conferences for their career benefit. This creates a lot of frustrations, because the acceptance rate is decreasing and there is no specific explanation for why the papers are rejected. We need support for small conferences; financial, promotion, etc... to promote these conferences better. Having journals like CiC is a good thing to solve the problem of “flagship” conferences being overcrowded. Overall, there is a cultural bias against conferences that are not “flagship”; while it’s more difficult and tricky for the careers of young researchers, some senior researchers are not supportive of publishing in small conferences even though they are the people who have the option of supporting since they already have a secure job position. Some senior researchers are also not supportive

of small conferences due to wanting to help their students in their career.

☞ **Demand 2:** IACR should promote and potentially sponsor smaller conferences and make well-established IACR-affiliated events into IACR venues, especially those outside of North America and Europe (i.e. LATINCRYPT, AFRICACRYPT, INDOCRYPT).

☞ **Demand 3:** Improve inclusion measures at conferences by providing period products and having gender-neutral restrooms as an option.

Life as an International Researcher Some countries have a security background checks for hiring. Some countries of origin makes it way more difficult for the check to pass. The applicant can be denied for no specific reason, and puts the denied researcher in a precarious situation. Indeed, without working abroad, your visa might not get renewed and you might be forced to leave the country. This puts loads of stress on the researcher, and might require them a lot of time and effort to appeal the decision. In some cases, these background checks don't make much sense as the subject can be very theoretical and not sensitive at all.

The administrative work for international students and researchers can be a massive burden. It is very difficult to gather information when moving to a new country, especially when the majority language (or official language) is not your mother tongue. Sometimes, people seek help from colleagues and labmates, but they might not find the information that they need because their coworkers are citizens and do not need the same paperwork. To settle down in France, one might need to ask a coworker or even a supervisor to be their "garantor", this needs transmission of very personal documents, which might be uncomfortable for both parties. There are some websites like <https://www.dossierfacile.logement.gouv.fr/> that do a good job verifying and watermarking documents, but very few people are aware of it, especially if they have recently moved to France (disclaimer: it's a government-based website). Chicken and egg situation: sometimes you need A to get B, but you also need B to get A. Example: having a French bank account needed to rent an apartment, but you need a French address to have a French bank account...

☞ **Sparked Initiative:** a centralized visa and paperwork resource platform (a community-maintained wiki from where people can get informed about asking for visas based on their passport, as well as settling down in different cities/countries).

Suggested Community Effort: talk about our demands and efforts at rump sessions, IACR membership meetings, and in-person during venues that we go to. This provides an easy way to get visibility, also since the IACR representatives are there, they get aware quickly and more interactively.

Working Group 3: Disabled Cryptographers (In-Person) People with disabilities are often stigmatized and not accommodated enough by our society, additionally fueled by a lack of information and stigmas around the many types of disability. We believe that this topic is rarely discussed, despite having a big impact on affected persons, and deserves more space. Our discussion focused on our experiences and challenges with our disabilities, identifying accommodations that would help us, and creating a small community space, dubbed the “Disabled Cryptographers Collective”.

Disability in Cryptography – Challenges The term *disability* is often connected with the symbol of a man inside a wheelchair. However, many disabilities are *invisible*, i.e., one cannot directly identify a disabled person as being disabled. For example, mental health issues or many other diseases which are not as visible as, e.g., a broken arm, often go unnoticed by others. Looking at the population in France, there are around 11% officially recognized disabled workers (DREES 2023), but it does not “feel” like it. Nonetheless, these disabilities affect us, but their invisibility leads to them often staying unaddressed in our workplace or in other spaces. Even worse, we sometimes have to argue that we are actually disabled, since some people refuse to believe a “healthy-looking” person to have a disability.

Moreover, there are stigmas surrounding disabled people, different kinds of disabilities are received differently and as such, are accommodated differently, if at all. For example, neurodiversity is more diverse than the stigma of the “superfunctional” autistic man. Neurodiverse people often additionally struggle with Depression or Anxiety, on top of navigating a world built for neurotypicals. Since everyone experiences living with their disability differently, disclosing what is up and how it manifests for one is a lot of extra work for us. We have also realized throughout our discussion that the criteria for the receiving an official “Disabled Status” differs across countries and many of us lack important information on how to get such a status and what impact this status may have.

As women, we already feel that we “ask for more” in our workplaces. Adding our disabilities on top makes us hesitate to ask for “yet even more”. Now a discussion on whether an invisible disability is there or not (for example because we want to negotiate possible accommodations) is made additionally harder for us to navigate with gaslighting, micro-aggressions, or simply not being taken serious enough.

Ideas for Possible Accommodations We have discussed potential ideas which could help us manage our disabilities better:

- Take meetings only in the afternoon (or morning) to take pressure off yourself.
- Schedule meetings only from 9am-11am / recorded and with notes so people are in the loop even if they cannot make it
- Group meetings together to avoid getting stuck in “waiting mode” in-between.
- Flexibility to rearrange meetings.
- Take a day off if you don’t feel well but not having to share if you don’t want.

However, we have seen throughout the discussion that coming up with a definitive “list of possible accomodation” (e.g., specialized for ADHD) is hard, because your mode operandi might change over time. Some strategies like moving meetings to certain time slots or grouping them might work for a while, but they could also need some adjustment later on again. Here, we have found that trying to keep in touch with ones own needs and having flexibility in our work places were key.

As a final useful tip, we discussed creating ones own Code of Conduct along the lines of a *How to Deal with Disabled People* for unaffected people. The idea was to briefly explain ones own disability and how it affects ones (work) life.

Conclusion Our key takeaways were the following: We need more awareness and remove the stigma surrounding people with disabilities. Moreover, collecting more information on what oppourtunities are available for us and what you can make use of.

✿ **Sparked Initiative:** We have also created a Discord channel which should serve as a space for cryptographers with disabilities of any form or kind, for instance, physical disabilities, mental illnesses, and neurodivergence. The main purpose of this channel is to share our experience in our work lives, personal lives (if one feels comfortable sharing of course!), and to support each other!

→ If you want to join, send an email to neurodiversityincrypto@gmail.com!

Suggested Community Effort: Organize small events and workshops within the Disabled Cryptographers Collective that are low-energy to attend, for instance online. Create further information for other cryptographers, e.g., through posters or rump session talks at IACR events.

2.7 Free Time

In addition to our official program, we offered multiple activities for participants to mingle in a casual way. It started with a very nice get-together in the old town on Monday evening for those who have already arrived to Montpellier. It was the occasion to meet the first speakers, panelists, and people from the different organization teams. On Tuesday, we organized a wine-and-cheese reception to jointly conclude the first day of the summit. On Wednesday afternoon, we organized through the tourist office of Montpellier an interactive guided tour through the city center.

And on Thursday evening, we made a trip to the beach in the south of Montpellier, to flee the hot city and cool down a bit. Beyond those in-official offered activities, participants organized dinner and other social activities together.



Fig. 6: Photos of the free time activities, taken & edited by David Haas.

3 Participation & Financial Report

For transparency as well as helping future editions, we provide in the following a concise financial report of the DDS as well as concrete numbers of participants.

3.1 Participation

In our planning, we expected 30-40 in-person participants and planned with at most 50. Overall, we had 29 in-person registrations (via the website) and 47 online registrations (via a google form).

From the in-person registrations, everyone who signed up also showed up, but not evenly throughout the 4 days. On average we were around 20/25 people in the auditorium, with stronger attendance at the beginning than at the end. From the

online registrations, we only had around 5 active participants. We are still trying to understand where the big delta came from.

3.2 Budget

The DDS'25 was financially supported by public money only. We received a national support of 1k€ by the Informatics institute of the CNRS (<https://www.ins2i.cnrs.fr/en>), a regional support of 2.5k€ by the ICO (<https://www.ico-occitanie.fr/>), and a local support of 1.5k€ by the LIRMM. The money by ICO, CNRS and LIRMM was managed through the LIRMM. We also received a support of 5k€ on reimbursement basis from CROSSING (https://www.crossing.tu-darmstadt.de/crc_1119/index.en.jsp). This gave us a base budget of 10k€. We also asked relatively high in-person registration fees, 352€ full prize and 198€ reduced price. Online participation was free. In practice only two third of the participants paid the registration fees, the others got them waived. We received roughly 5k€ through the registration fees, which gave as an overall budget of 15k€.

3.3 Costs

We didn't have to pay any fees for the auditorium and discussion rooms, as we were hosted for free by the university of Montpellier. The guided tour through the tourist office costed 425€. We booked two tours to have a capacity for 40 people. Given the number of people who participated at the tour, only one guided tour would have been enough, which would have divided the cost by two. As a caterer we took the university's caterer which was quite cheap and decent in quality. We paid ca. 2.4k€ for the (vegetarian only) lunches and coffee breaks. At the end of the first day we had a wine & cheese reception from a local caterer, which costed us ca. 700€. We printed in total 11 posters at the cost of ca. 400€. One lunch break we ordered pizza as the university caterer wasn't available at the cost of ca. 250€. We also did some small shopping at the supermarket (vegan milk and snacks, period products, etc) for ca. 200€. Through the LIRMM, we gave out several travel stipends, for an overall budget of 2k€. Among this was a flight for 600€ for one person who at the end didn't receive the VISA, so we lost that money. We also gave travel stipends on reimbursement basis through CROSSING for a total of 4.3k€, the delta of 700€ (from the 5k€ attributed to us) remained at CROSSING. Aarhus University paid the travel for one of our invited speakers, as she visited Aarhus University after the DDS'25. Sofia Celi paid the gathertown invoice (280USD) through her personal budget as reimbursement was tricky as the invoice was on her name. Next time, we should either pay it directly through the university's credit card (in French *carte d'achat*) or have the correct billing name and address for reimbursement. **At the end, ca. 2k€ remained at the LIRMM as a plus.**