IACR 2022 Election: Candidate Statement for Allison Bishop

I have been part of the cryptography community since around 2009, when I published my first paper on the topic. During my Phd at the University of Texas, I contributed to the development of the dual system proof methodology and co-authored many results in attribute-based encryption, leakage-resilience, and other topics. For some years after that, I was a faculty member at Columbia University, where I advised Phd students and continued to pursue cryptography research. I began to suspect that working solely in academia was holding me back from doing impactful research on a short or medium timescale, as I felt ill-equipped to imagine what the most useful problem statements would be. To learn more about computer science in practice, I sought out consulting work in industry. In 2016, I flipped from being a part-time consultant and full-time academic to be a full-time industry researcher and a part-time academic.

In 2019, I co-founded Proof Trading, a company that seeks to bring high standards of transparency and rigorous science to the financial services industry, specifically to the domain of institutional stock trading. I wrote a blog post here about how our company philosophy is inspired by the cryptography's community's rejection of "security by obscurity." My recent work also borders on cryptography at times, including forays into privacy definitions for financial data, and (so far incomplete) attempts to define a useful notion of computational indistinguishability for financial time series data. I currently teach part-time at City College, CUNY as part of their masters in cybersecurity program.

Also in 2019, I founded CFAIL, the Conference for Failed Approaches and Insightful Losses in cryptology. The intention of CFAIL is to provide a welcoming space for the discussion of ideas that contain valuable insights, even though they did not lead to publishable results in the traditional sense. CFAIL recently appeared in its fourth iteration as an affiliated workshop to Crypto 2022.

I have served on the IACR board for the last two years in my appointed position at Crypto 2022 General Chair. In that time, we have seen dramatic growth in IACR membership, as remote attendance at conferences become an option for the first time. In my role as a general chair, I sought to continue hybrid support for conference attendees and speakers, and to introduce novel programming elements aimed at community building.

I would like to continue serving on the board, and will advocate for continuing and increasing support for cryptographers who are unable to travel to IACR conferences due to challenges with covid, visas, costs, care-giving, and other constraints. I will also focus on how we can expand the available avenues for joining our community, and how we can better facilitate networking opportunities for young researchers in a world where in-person conference attendance may no longer be a default.

FAQs:

What have you learned from running CFAIL and Crypto? What might you do differently?

Four years of running CFAIL have taught me that there is a huge untapped well of creativity and humility in our community. One thing we're trying to figure out next is how we can lower the effort required to participate in CFAIL. One example might be moving to a submitted talk-based format instead of a paper/abstract-based format (e.g. more like RWC). We've also had at least one vote for changing the name to something more CV-friendly.

In terms of Crypto, I know we don't have the hybrid format completely figured out yet, but I think we can get there. There are a few things I could have (ahem, should have!) done differently to reduce the friction in switching between in-person speakers. These are already flagged for the next general chair and with the UCSB team for next year.

I also welcome the criticism that the women's networking event and allyship panel discussion should not have been at the same time. I was trying to balance many competing constraints, and I still feel I made a reasonable decision and that both events went very well. But I'm also glad to see the request for future single-programmed events of this type. I think we can and should do that in the future.

Have you ever run for an IACR board position before?

Yes. In the last election cycle, I ran for a director position. I lost by two votes. So please vote – your vote does matter! The results are actually quite funny (https://iacr.org/elections/2021/). For a CFAIL general chair, it was very on brand.

Who can vote in the IACR Election?

Anyone who is an IACR member.

How does one vote in the IACR Election?

The election is conducted electronically using Helios. You will receive an email invitation to vote.