The Interview Column

by

Chen Avin and Stefan Schmid

Ben Gurion University, Israel and TU Berlin, Germany
{chenavin,schmiste}@gmail.com

KNOW THE PERSON BEHIND THE PAPERS

Today: Shweta Agrawal

Bio: *Shweta Agrawal is an associate professor at the Computer Science and Engineering department, at the Indian Institute of Technology, Madras. She earned her PhD at the University of Texas at Austin, and did her postdoctoral work at the University of California, Los Angeles. Her area of research is cryptography and broadly theoretical CS, with a focus on post quantum cryptography. She has received several awards and honours such as the national Swarnajayanti award, the ACM India award for Outstanding Contributions to Computing by a Woman, a best paper award at Eurocrypt, best reviewer awards for Asiacrypt and CCS, invited speaker and program co-chair at the flagship conference Asiacrypt.*

EATCS: We ask all interviewees to share a photo with us. Can you please tell us a little bit more about the photo you shared?

SA: This picture is with my pet Tara, during one of our morning walks. This is a daily event so the picture is not special in the sense of being rare. But it shows how ordinary can be so fun!

EATCS: Can you please tell us something about you that probably most of the readers of your papers don't know?

SA: I love all kinds of art – music, painting, poetry, literature, sculpture, ceramics and anything else. I pursued painting (oil on canvas) quite seriously for several years and had the beginnings of a career there (via some initial exhibitions of my work) before I ended up dedicating most of my time to academia. I think I love math because I see it also as a kind of art. I see beautiful connections between cryptography and abstract expressionism – both are playing with the boundaries between structure and randomness, form and formlessness! I also love to hike, and find myself in the Himalayas every summer.

EATCS: Is there a paper which influenced you particularly, and which you recommend other community members to read?

SA: When I was in graduate school, the first paper on fully homomorphic encryption by Craig Gentry [2] came out. This paper had a very significant impact on me.

It was such a beautiful, simple to state problem, and the solution was so creative. A series of subsequent works (also very cool) improved this significantly, but the first paper was always special to me. It was so surprising – it broadened for me

the landscape of what is possible. I have always loved the apparent paradoxes in cryptography and this paper was a wonderful example.

EATCS: Is there a paper of your own you like to recommend the readers to study? What is the story behind this paper?

SA: I think the paper on obfuscation from Eurocrypt 2019 [1] is my paper that I like the most. I loved the problem – the balancing between algebraic structure and computational hardness was so delicate and beautiful! In this paper, I made new conjectures about hard lattice problems and this was a very mixed experience. On one hand, I love exploring such questions, on the other, it also gave me many anxious days and sleepless nights. I sat on this paper for a whole year before finally posting it online – I was so nervous about the conjectures. I used to joke that I love it on odd dates and hate it on even. Finally, a casual conversation with a colleague (Daniele Micciancio) is what helped me make it public – he remarked something to the effect that if my conjectures survive (algorithmic attacks), it's great, if they are broken, then I'll still be in good company. He was referring to the fact that several conjectures made by eminent researchers in the space of obfuscation had been broken. I decided it was worth putting out there for people to look at.

EATCS: When (or where) is your most productive working time (or place)?

SA: Early hours of the morning are the best for me. Place does not matter too much – after Covid, I've become relatively robust to this aspect and can work from anywhere. That said, quiet walks in green places where I am not actively thinking about any problem, but just letting "the cooking pot" simmer in my head, are the most productive. For me, most good ideas come when the mind is relaxed, typically when not working actively. I am fortunate to live in a very beautiful area with gorgeous, seemingly timeless banyan trees all around. While summer is very hot where I live, there is also a wonderful, stark beauty to it. The bright yellow of the sun filtering through the thick green foliage of the banyans is magical. I suspect that every good idea that I have ever had was somehow born here.

EATCS: What do you do when you get stuck with a research problem? How do you deal with failures?

SA: I try to have clarity on why the techniques I am trying are not sufficient for the problem I am working on. By identifying a fundamental roadblock which is not allowing me to proceed, I feel that I have understood the root cause of the issue and this helps me to get closure. At a philosophical level, I try to not be too obsessed with the outcome of the effort – at a deeper level, one is in this field for the beauty of it, and grasping too much at particular desired results ruins that. So stepping back and focusing energy on something else (inside or outside science)

helps. Having dealt with a large number of failures over the years also helps – one is able to internalize that life really does go on and there are many other questions to study.

EATCS: Is there a nice anecdote from your career you would like to share with our readers?

SA: Perhaps the most significant thing I can share is from the time when I started the process of moving back to India after my postdoc, which (together with my PhD) was in the US. I had always wanted to contribute to science in India – my growing up years in India had been in an environment of enormous struggle and strife, set in a canvas of equally enormous kindness and generosity. In this environment, I had somehow managed to get the best of opportunities that any girl could have, anywhere in the world. It was my deepest desire growing up, to somehow give back to where I came from, in whatever small way I could.

While I had always been certain I wanted to do this, I had a bad case of cold feet as the time started approaching. During my PhD and postdoc, I had worked in groups that were among the best in the world, and had always been surrounded by super smart, highly trained and extremely motivated people. The momentum of the group had always been a big factor in my own progress, and I was very nervous about whether I could do any meaningful research without such a support structure – back then there was almost no one working in my area in India. To add to it, people that I held in very high regard made comments about how this move was essentially professional suicide, and this shook my already shaky confidence even further.

Yet, I made the move and things worked out. Being without the support of the group structure forced me to become more independent and get clarity on my own research agenda. I believe my work has become more authentically my own and hence deeper, and it has been very satisfying to be able to live my childhood dream. Looking back, I'm glad I did not give in to the worries and fears of that time!

EATCS: Do you have any advice for young researchers? In what should they invest time, what should they avoid?

SA: I think the main "advice" I have (this makes me feel old!) is to be unapologetic about being yourself and to work on questions that you love. Invest time in taking courses, learning new things, attending talks and asking lots of questions. When trekking up a mountain, one enjoys the beautiful views along the way. Research is the same – the tedium of the climbing should not get in the way of the enjoyment. If one dedicates one's effort to something unshakeable, like beauty or service or anything broader than oneself, then it is easier to keep going when frustrations and failures come (as they inevitably will).

One should avoid comparing oneself with others, or falling into negative self talk and such other habit patterns. We feel best and do best by being ourselves, not anyone else – no single colour is the most important in a painting. I remember thinking for one painting (by Cezanne, I believe), how a single streak of a particular green (viridian), which was not present anywhere else in that painting, was foundational to its beauty. One must ruthlessly negate the desire to be like anyone else.

EATCS: What are the most important features you look for when searching for graduate students?

SA: I try to separate ability and "spark" from training. Often students come in who haven't had the opportunity to get very rigorous training yet – this is something that can be fixed, given time. What is more innate is their ability, enthusiasm, motivation and earnestness. I've been very lucky in the students I have had so far. I also think that as an advisor, one can play a big role in shaping innate qualities and helping to develop weaker aspects. So I try to keep a very open mind.

EATCS: Do you see a main challenge or opportunity for theoretical computer scientists for the near future?

SA: Science is constantly evolving and each era brings wonderful new questions. Being a cryptographer, one area I am very excited about is quantum algorithms and their effect on cryptography. We understand so little about computational hardness in cryptography even in the classical regime and asking questions about hardness in the realm of quantum is really intriguing. I am excited to see what quantum algorithms can do to solve problems that we consider difficult classically.

EATCS: Can you recommend some source of information that you enjoy (e.g., a specific blog, podcast, youtube channel, book, show, ...)?

SA: I enjoy reading, particularly Indian philosophy, history and popular science. A favourite in the popular science category is "The fabric of the cosmos" by Brian Greene. I love poetry deeply – a favourite here is Seamus Heaney's "Clearances". Another book I recently enjoyed a lot was "Consolations" by David Whyte. A great source of inspiration for me is painting – I am blown away by the works of Jackson Pollock, M.F Hussain, Hans Hoffman and Picasso. The pinnacle of brilliance and beauty for me are the verses of some of the old Indian philosophy texts like "Katha Upanishad" and "Yoga Vashishta".

Please complete the following sentences?

- *Being a researcher* is a great job – so much freedom and space!
- *My first research discovery* gave me the confidence that I could do this.
- Having good intentions *is key to being a happy academic.*
- *Theoretical computer science in 100 years from now* will be just as rich and beautiful!

References

[1] S. Agrawal. Indistinguishability obfuscation without multilinear maps: New techniques for bootstrapping and instantiation. In *Eurocrypt*, 2019.

[2] C. Gentry. Fully homomorphic encryption using ideal lattices. In *STOC*, pages 169–178, 2009.