Podcast Name: *ACM ByteCast*
Episode: Episode 47 - Yael Tauman Kalai

Welcome to the *ACM ByteCast* podcast, a series from the Association for Computing Machinery! The podcast features conversations with researchers, practitioners, and innovators at the intersection of computing research and practice about their experiences, lessons learned, and visions for the future of computing. In this episode, host Bruke Kifle interviews guest Dr. Yael Tauman Kalai.

Dr. Yael Tauman Kalai's research has advanced the theoretical foundations of cryptography and influenced practical applications with many implications. She is the Senior Principal Researcher at Microsoft Research and an adjunct professor at MIT. Her main research interests are cryptography, theory of computation, security, and privacy. She is especially known for her work in verifiable delegation of computation, where she has developed systemic proofs that certify the correctness of any computation. Her proofs have been useful in areas such as Blockchain and cryptocurrency. She has received many prizes including the 2022 ACM Prize in Computing.

To begin, Dr. Kalai shares about her own career journey. She studied mathematics during undergrad and loved the subject deeply. However, she eventually found that she couldn't find a specific problem in her research that excited her the way computing did. The field of computer science offered her an engaging way to practice mathematics and have real world impact. What she loves most about cryptography is that its questions are philosophically interesting and widely applicable. Cryptography, Dr. Kalai explains, has traditionally been a way of securing communication. In today's digital world, it has changed to involve securing both computations and communication through privacy and integrity. Next, Dr. Kalai shares her process for coming up with innovative solutions to problems. Observation is usually the way she arrives upon the problems she wants to solve. The solutions usually appear when she is in a period of obsession about solving a certain problem. Within the realm of computer science, there are so many ways to conduct research.

Dr. Kalai is attributed as co-inventing ring signatures, which allow a member of a group to give anonymous comments digitally. Her paper on this research is entitled *How To Keep A Secret*. With ring signatures, messages can be sent on behalf of yourself (or someone else) without revealing who the sender is within the group. This can raise some serious questions regarding authenticity and whistleblowing. Blockchain companies used ring signatures to introduce piracy to the chain. Dr. Kalai reminds listeners that the majority of her projects require a team of people who are willing and interested to solve the same problem. She tends to place value on her research by evaluating its real-world usability.

Before wrapping up, Dr. Kalai shares about her experience working in academia vs. industry. She highlights Microsoft Research as an amazing and supportive place to have her lab. She also enjoys seeing the spark in her students' eyes when they find the area they are interested in. She feels that she is able to have the best of both worlds with the like-minded students at

MIT and the diversity of her colleagues at Microsoft. In closing, she speaks to the concerns around the growth of quantum computing. Now, the industry is working hard to ensure that cryptography is post-quantum secure. On the other hand, quantum computers present lots of positive promises. Finally, hear what she is most excited about looking towards the future of the field.

Key takeaways:
2:15 - Dr. Kalai shares about her career journey.
9:48 - What is cryptography and why is it important?
16:25 - Explaining different methods of verification.
29:18 - AI and large language models.
35:35 - Dr. Kalai's work regarding ring signatures and its practical applications.
42:00 - How Dr. Kalai values her own research work.
46:20 - Balancing the roles between academia and industry.
54:25 - Concerns around quantum computing.
59:40 - The most exciting emerging areas of cryptography.

Links
Learn more about Yael Tauman Kalai.
Learn more about Bruke Kifle.
Learn more about the ACM ByteCast podcast at https://learning.acm.org/bytecast

Tags:
Data security, computing, privacy, cryptography, blockchain, cryptocurrency, computer science, security and privacy, authentication, problem solving, AI, artificial intelligence, language models, data, cryptographer, ring signatures, mathematics , microsoft, research initiatives, machine learning, theory, NIST, quantum security, quantum computers, cybersecurity