IIT Chennai Swarnajayanti Fellow to improve algorithms in lattice cryptography—an emerging technology for secret keeping

Dr. Shweta Agrawal from Indian Institute of Technology, Madras, Chennai, is one of the fourteen recipients of this year's Swarnajayanti Fellowship instituted by Govt. of India to commemorate India's fiftieth year of Independence. The prestigious fellowship is funded by the Department of Science & Technology.

Using the Swarnajayanti fellowship, Dr. Agarwal would like to conduct a deep study on one of the most promising approaches for post quantum cryptography, namely, lattice based cryptography to improve algorithms and understand gaps between theory and practice. Lattice based cryptography which is resistant to attack by both classical and quantum computers is the leading candidate for post quantum cryptography and design of a cryptographic system for the future.

Cryptography is a beautiful branch of theoretical computer science that seeks to provide guarantees to the art of secret keeping. This field elegantly balances itself on the tightrope of mathematical beauty on one side, and practical importance on the other. The scientific charm of this field lies in the deeply paradoxical questions it poses.

The simplest goal of cryptography is to hide information so that learning a message from a cryptographically sealed envelope implies a solution to some well known mathematical problem. By suitably choosing the underlying mathematical problems to be difficult, we may rest assured that an attacker's chances of learning secret information are extremely small.

Typically, an attacker is modeled as a classical computer. However, recent times have seen significant advances in the construction of quantum computers, which are based on the laws of

quantum rather than classical physics. Most modern-day cryptography relies on the difficulty of problems which, while difficult for classical computers, are efficiently solvable by quantum computers. Thus, most modern-day cryptography breaks down if quantum computers are used by the attacker.

A few weeks ago, Google claimed to have demonstrated "quantum supremacy," namely, construction of a quantum computer that can experimentally demonstrate a massive speedup over a classical computer. Soon after, Chinese researchers claimed that they expect to demonstrate quantum supremacy by next year. Thus, the advent of quantum computers has crossed the realm of scientific fantasy and looms as a real threat in the near future. Therefore, it is imperative to redesign cryptography ground up to resist quantum computers -- that is, to design post-quantum cryptography. This is the focus of Dr. Agrawal's work.

Developing expertise in post-quantum cryptography is of national importance. Aside from its practical importance, this is a rich and emerging area of cryptography, and construction of state of the art systems in this field can significantly enhance the visibility of India in the global arena. Not only does her proposed work help create intellectual property, but it also creates expertise within the country that will lead to intelligent post-quantum cryptography design for the use of our government, military, industry and society alike.

In her current work, Dr. Agrawal has provided constructions of advanced cryptographic protocols that are believed to be resistant to quantum computers. She has particularly focused on the emerging field of 'computing on encrypted data' which may allow (for instance), machine learning algorithms to be run on encrypted genetic data, leading to advances in the field of personalized medicine. Such algorithms, if realized efficiently, can have wide applications in areas as diverse as medicine, governance, social sciences, and many others, leading to an elegant synthesis of disparate sciences.

This is a very young field, and there are significant gaps in the understanding of this area. Her research agenda is to tackle fundamental questions in lattice based cryptography, to endeavour to fill in these gaps. She hopes to create national expertise in lattice based cryptography that will benefit society by creating knowledge and applications alike.