# A MATHEMATICS HUB FOR A POST-QUANTUM WORLD

FROM TACKLING POST-QUANTUM CRYPTOGRAPHY to evaluating software for simulations, this emerging mathematics institute in central China is supporting researchers in basic and applied mathematics.

**While quantum computing has vast potential,** it could also threaten cybersecurity. "Current encryption methods are less secure in the face of the superior computation power of quantum computing" says Tianze Wang, director of the Institute of Mathematics at the Henan Academy of Sciences in China.

Before quantum computing becomes ubiquitous, researchers led by Wang are rushing to develop 'post-quantum cryptography' for enhanced cybersecurity.

Established in 2021, the Institute of Mathematics is based in Zhengzhou, a city on the banks of the Yellow River that was the capital of China three millennia ago.

Since its launch, the institute has received strong support from the government in terms of resources, funding and talent. "It is a critical part of this province's overall goal to rebuild and revitalize the Henan Academy of Sciences," says Wang. "Ultimately, we want to build a major centre of innovation and talent for mathematics."

MF3d/iStock/Getty

▲ **Mathematicians in Zhengzhou, China, are working on a new encryption system to mitigate cybersecurity risks in the looming era of quantum computing.**

## STIMULATING POTENTIAL

The institute has already established talented teams in number theory and cryptography, and intelligent computing, to address major fundamental mathematical problems and generate real-world applications. A top priority is the post-quantum encryption system called 'Fully Homomorphic Encryption'.

"This new encryption system is closely related to number theory and algebra in basic mathematics," explains Wang, who has been deeply engaged with number theory for the past 30 years. Working with renowned mathematician, Jingrun Chen, in the 1990s, Wang contributed to Goldbach's Conjecture, which asserts that every even integer greater than 2 is the sum of two prime numbers, and which remains unsolved today.

The institute's positive research environment allows researchers to thrive, says Ruili Wang, a computational mathematician in the Intelligent Computing Team. "We can tailor our project to our strengths, so that we can devote ourselves to research," says Wang, who left a lengthy post at the Institute of Applied Physics and Computational Mathematics in Beijing to move to Henan.

Ruili Wang is developing a new tool to evaluate the effectiveness of engineering simulation software, which researchers use around the world to simulate real processes, such as those observed in ocean waves, hurricanes or combustion. This type of software combines physical models, mathematical methods, computer technology, and engineering knowledge, but it also involves a lot of uncertainty, says Wang.

## MEASURING UNCERTAINTY

The uncertainties could come from input parameters, experimental measurements, or other variables. In the past few years, Ruili Wang and his colleagues have been quantifying these uncertainties to determine how much they affect the software's modelling outcomes. "Now, we are translating our quantification theories into software that we use to assess whether this engineering software is real, reliable and stable," he says.

The institute continues to welcome early career researchers focusing on algebra, geometry and analysis from universities and research institutes such as Nankai University in China, the Chinese Academy of Sciences, and the University of Cologne in Germany. These collaborations provide a solid foundation for long-term cooperation and exchange.

"Our vision is to ultimately become a base for training high-level researchers, and to contribute to the development of mathematics and applied mathematics in Henan Province and even in central China," says Tianze Wang. ■

www.hnas.ac.cn/sxyjs/
sxs-gkzp@hnas.ac.cn