UC SANTA BARBARA

THE Current

March 2, 2026
Cameron Walker

Could quantum computers protect privacy and security?

Whether you use a smartphone or a computer, pay for things with a credit card or go to a doctor who uses electronic medical records, you rely on the layers of security brought to you by cryptography. Many in the cryptography world are concerned that this security will be threatened by a future in which quantum computers could potentially crack open access to sensitive data. But what if quantum computers could help protect privacy and security instead of jeopardizing it?

That's what UC Santa Barbara computer science associate professor Prabhanjan Ananth is focusing on as part of a new National Science Foundation grant. The three-year, $300,000 grant will fund Ananth's work, which is aimed at understanding theoretical aspects of quantum cryptography that could be used to protect computing in the future. Quantum cryptography is relatively less explored than post-quantum cryptography, which uses classical systems to repel quantum computers. "I want to understand if there are any positives that we can exploit from quantum computing," he said.

"Quantum computers that are able to break many of the existing cryptographic schemes are quite likely to be available in the not-too distant future, so it is urgent to be able to build cryptographic schemes that are resilient to quantum attacks," said Daniel Lokshtanov, computer science professor and vice chair of the Department of Computer Science. "At the same time quantum computation allows us to construct schemes that are probably impossible with only classical computers, and it is equally important to understand these. Our department is very fortunate to have Prabhanjan Ananth among its faculty, as he is doing absolutely cutting edge research in this space."

From classical to quantum cryptography

Ananth, who received his Ph.D. at UCLA and studied cryptography as a postdoctoral researcher at MIT, arrived at UCSB in 2019 knowing he wanted to branch out into quantum cryptography. But as a new professor, "It seemed like a risky move," he said. "But I really liked linear algebra, and as I read about quantum computing, I realized I really wanted to explore this. There happened to be some very interesting problems at the intersection of quantum computing and cryptography, so I started working on those."

Classical cryptography relies on mathematics-based cryptographic assumptions, which are extremely challenging problems that are hard to solve using efficient algorithms — for example, factoring a number that is a product of two large primes. These assumptions, called cryptographic primitives, establish a baseline of privacy and security, and cryptographers use multiple primitives as building blocks to construct a resilient security system.

In recent years, researchers have been proposing and developing many quantum cryptographic primitives — which use quantum mechanical principles as their foundation — with the potential to be used for building secure systems.

That's where Ananth and his colleague, co-PI Henry Yuen at Columbia University, come in. Together, they will study new primitives that are being proposed, and compare them to existing primitives. "We want to understand if certain primitives are stronger than others, what sort of computational assumptions are needed, what are the running times of these primitives and so on," Ananth said.

Their goal is to establish a hierarchy of different quantum cryptographic primitives to answer questions such as which primitives would provide the best security and which ones could work together in a cryptosystem. Along with building the hierarchy, Ananth said, the team hopes to discover new cryptographic tools that rely on quantum mechanics. For example, information in a quantum system cannot be copied; cryptographers could harness this no-cloning principle to enhance security.

This is not the first time NSF has funded Ananth’s research on quantum cryptography. In 2023, he received a three-year, $300,000 award to study the theoretical foundations of quantum pseudorandomness primitives. While quantum computing relies on the unpredictability of quantum states, it can be costly — and in some cases, impossible — to develop truly random systems. Pseudorandom states can mimic randomness but are easier to work with, and through this particular award, Ananth is looking at the potential usefulness of pseudorandomness in cryptography.

In 2024, Ananth received a five-year, $665,000 NSF award for his research on unclonable cryptography. “This is an area of quantum cryptography that leverages the foundational principles of quantum mechanics to build secure cryptographic systems that are probably impossible to build using existing technology,” he said.

Using his broad background in quantum approaches to cryptography, Ananth hopes to ultimately generate the hardest possible problems for future hackers to solve. “We want to make the life of the malicious actors as hard as possible,” he said, adding that the journey continues. “We haven't reached a point where we can say, this is the best, hardest quantum-inspired problem we can pose. That’s what I'm setting out to do.”

Tags
Quantum Science

Media Contact
Shelly Leachman
Editorial Director
(805) 893-2191
sleachman@ucsb.edu

About UC Santa Barbara

The University of California, Santa Barbara is a leading research institution that also provides a comprehensive liberal arts learning experience. Our academic community of faculty, students, and staff is characterized by a culture of interdisciplinary collaboration that is responsive to the needs of our multicultural and global society. All of this takes place within a living and learning environment like no other, as we draw inspiration from the beauty and resources of our extraordinary location at the edge of the Pacific Ocean.