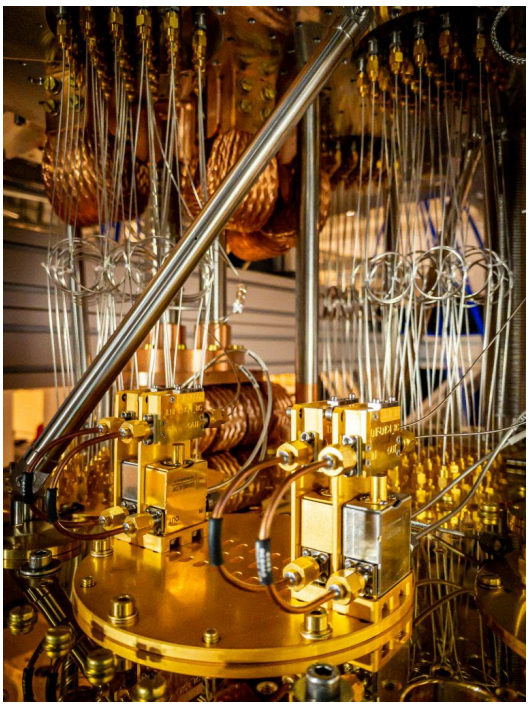
Securing Real-Time Communication in a Post Quantum World

Advances in Quantum Computing are placing the encryption algorithms and protocols that protect everything from commercial banking to defence grade communications services at risk. What steps are needed to protect future communications and is simply adopting PQC enough?

Post Quantum Cryptography (PQC) was one of the hot cybersecurity topics last year and 2025 will be no different. Back in 1994 Peter Shor, now a professor at MIT, published an algorithm for finding the prime factors of an integer. While this may sound like a topic of limited interest, factoring large integers forms the foundation of many of the cryptographic protocols in use today. Generating large prime numbers is easy. Multiplying two large primes to get an even larger number is also easy. The whole process can be completed in fractions of a second. The reverse process, factoring a large number to recover the component primes is computationally very difficult. The process can take billions of years on even a powerful traditional computer. This asymmetry is exploited in algorithms such as RSA and Diffie-Hellman to implement key generation and key exchange protocols. Two systems wishing to protect information exchange can establish a shared key for data encryption. An attacker monitoring the encrypted data exchange will not be able to reconstruct the encryption key in any useful timescale.

Shor's algorithm changes all this. The algorithm can factor a large number in seconds. An attacker can exploit Shor's algorithm to recover an encryption key and read the content of a captured data transfer in near real-time. Shor's algorithm is a quantum algorithm that runs on a quantum computer.



Credit: Berkley Lab

As of the start of 2025 quantum computers large enough or stable enough to run Shor's algorithm and recover an encryption key of realistic length do not exist. However, with advances in quantum research, it is likely that a suitable quantum computer will exist in the next 5-10 years. This poses the real risk of *harvest now, decrypt later.* An attacker can monitor encrypted communications today and save the captured data for decryption in the future. If the information exchange in a communications session needs to be protected for 5 years or more, then action needs to be taken now to ensure future security.

Fortunately, the security community has not been idle. There are now a number or replacement algorithms that are secure against a quantum computer attack and provide effective Post Quantum Cryptography. Three of the algorithms have been registered as FIPS standards. There is now a rush of software vendors announcing support for PQC.

Despite the excitement over PQC, it is not the complete answer. Firstly, the quantum threat affects only asymmetric encryption algorithms (public/private key algorithms). These algorithms play an important role in setting up encrypted communication including securely establishing a shared key for bulk data encryption with a symmetric algorithm. Symmetric algorithms such as AES are not compromised by a quantum computer attack. Secondly, encryption is only one component of a security policy, although an important one. Encryption must be combined with defences against a range of threats. An attacker targeting an encrypted voice or video call is likely to target the communication endpoints and monitor the audio/video streams after they have been decrypted for playing to the end-user.

UM Labs specialises in securing standards based real-time communication. Unicus®, the company's security platform, is designed to protect standards based real-time communication services on IP networks. This includes voice and video calls, static and mobile surveillance covering body cameras, drones and fixed cameras, cloud extended reality (CXR) services and IoT applications ranging from simple monitor/actuator systems to complex remote control applications. Unicus implements a layered security policy with a core/edge architecture ensuing that all endpoints of a real-time communications network are protected. Both edge and core components include PQC providing encryption to meet elevated security requirements in a post quantum world.

UM Labs is at DPRTE in Farnborough on the 26th and 27th March, come and see us on stand 136, visit our website at www.um-labs.com or contact us at info@um-labs.com.