

# QuSecure Unveils Quantum-Resilient Communications Satellite Link

Quantum cybersecurity firm QuSecure has announced the first known end-to-end quantum resilient encrypted communications link via satellite. It protects data delivered by satellite from classical- and quantum-computer decryption.

The journey starts at Quark (QuSecure Orchestrator). Quark is described as the brain of the QuSecure solution and is the key distribution platform. The philosophy is to provide absolute agility. It supports all NIST recommended post-quantum algorithms, and can interface with any quantum random number generator (QRNG). This is where the keys are generated.

Quantum agility is important. Nobody expects the recommended algorithms to last forever – the likelihood is that some, if not all, will eventually fail. They will need to be replaced by other or new or simply stronger algorithms. Agility implies an effortless ability to switch from one algorithm to another, as necessary or simply desired.

“We support the entire suite of [NIST] finalists,” co-founder and CPO, Rebecca Krauthamer, told *SecurityWeek*. “It’s all just a policy configuration and it’s very simple.” Currently, QuSecure defaults to the Quintessence quantum random number generator, and the Kyber algorithm.

The keys are delivered to QuEverywhere via a QSL tunnel, which adds quantum resiliency to TLS. QuEverywhere was launched in January 2023. It is described as the first quantum-safe orchestration solution protecting encrypted private data on any website or mobile application with quantum-resilient connections and sessions, all with no end-user installation required.

The latest development now announced is that this quantum resilient link can be extended to satellite communications – meaning the link between an end user and, for example, a website will be quantum resilient even via a satellite connection. This is important since air-borne data traffic can be sniffed and is, if anything, more susceptible to the ‘harvest now, decrypt later’ threat.

“QuSecure’s breakthrough in secure satellite communications capabilities creates the world’s first extraterrestrial post-quantum resilient communications mesh; and is a very important step in our collective journey toward quantum safety,” said Aaron Moore, QuSecure’s EVP, Head of Engineering.

Quantum-resilient cryptographic communications satellite link via Starlink

The importance goes beyond the need for secure commercial communication – government and military are also strong users

of satellite communications. “This enables servers, edge, IoT, battlefield, and other devices outside conventional data networks to adopt quantum-safe communications,” says QuSecure.

For its satellite test, QuSecure used the Starlink low earth orbit (LEO) satellite network. Quantum resilient data was sent from Quark through labs at Rearden Logic in Colorado to a Starlink terminal. From there the data was uploaded to a Starlink satellite, and then delivered via downlink back to earth.

The choice of Starlink may seem obvious simply because of the quantity of satellites in orbit – but is also important because of the redundancy that this provides. Consider, for example Russia’s first action in the current phase of the Ukraine war – an attack against the Viasat satellite communications system. Musk stepped in and provided Starlink to Ukraine to maintain internet connections.

Attacks against this quantity of satellites becomes infeasible, and less likely given that an enemy could intercept airborne data with the possibility of decrypting that data. However, given the combination of Starlink’s inbuilt redundancy and QuSecure’s post-quantum resilient capabilities, the likelihood of an enemy intercepting and decrypting wartime communications – even if or when they have quantum computers – becomes unlikely. These same strengths can be used by any commercial organization for any commercial application.

“Because we are software-based and don’t need hardware on every single satellite, there is no single point of failure in our system,” added Krauthamer. “We can failover to another Starlink satellite and potentially another orbit where the communication will seamlessly continue to operate without disruption.” It’s an extension of the ‘agility’ concept, applied here to hardware rather than algorithms.

**Related:** Cyber Insights 2023 | Quantum Computing and the Coming Cryptopocalypse

**Related:** Is OTP a Viable Alternative to NIST's Post-Quantum Algorithms?

**Related:** The Promise and Threat of Quantum Computing

*QuSecure Unveils Quantum-Resilient Communications Satellite Link*