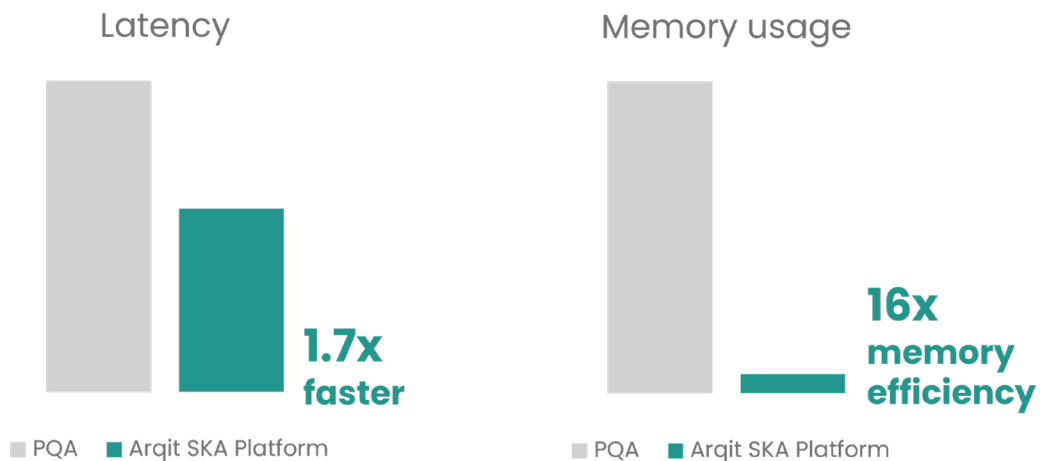




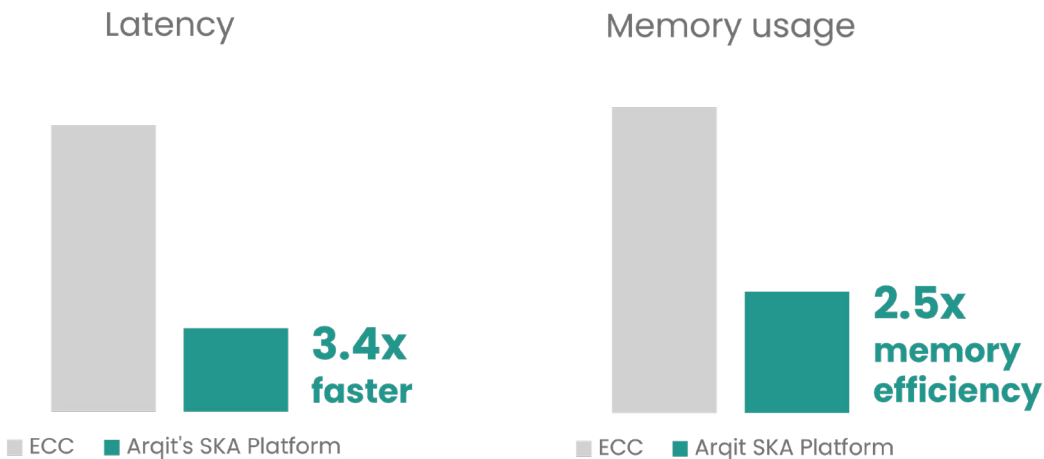
Arqit SKA Platform outperforms ECC and PQA

Arqit has established the performance benefits of our key agreement product through rigorous external testing. We found that measured latency and memory use of SKA Platform™; Arqit's symmetric key agreement platform, significantly outperformed equivalent key agreement mechanisms using Elliptic Curve Cryptography (ECC) and Post-Quantum Algorithms (PQAs).

Comparison with PQA



Comparison with ECC





Results

Key Exchange Algorithm	Latency (ms)	Memory use (kB)
Arqit SKA Platform	84.33	8,737
CRYSTALS-Kyber	143.07	143,140
Elliptic curve Diffie-Hellman	288.84	22,032

Method

Arqit compared the latency (the total time taken) and memory use (RAM resources) used to complete full authentication and key agreement between an initiator device and a receiver device. For PQA we used a combination of CRYSTALS-Dilithium-5 and CRYSTALS-Kyber-5 which are rated to have a security equivalent to AES-256, similar to SKA Platform. For ECC we used secp256r1.

- Measurements were made on two unmodified Raspberry Pi 3b+ boards connected with an ethernet cable to reduce the impact of Wifi fluctuations.
- We used the open-source library 'mbed TLS' as a TLS implementation, together with libOQS as the PQA implementation.
- We compared our algorithm with a combination of digital signature and KEM methods that have been selected as finalists in the NIST PQA competition, namely CRYSTALS-Dilithium for signatures and CRYSTALS-Kyber for KEM.
- We chose the parameter set for these which achieve NIST's Security Level 5, which is comparable with AES-256 security as offered by SKA Platform.
- We compared key agreement using PQA with creating a "bilocation key" using SKA Platform, i.e. a key that requires communication with SKA Platform.

Conclusion

These results show that SKA Platform is not only more secure than ECC and PQA but is also faster and uses fewer resources.

Numerical analysis of SKA Platform with comparable post-quantum cryptography (PQA) methods for authentication and key agreement show that **SKA Platform endpoints agree keys 1.7x faster and are 16x more memory efficient than PQA.**

In addition, similar analysis was performed which compared SKA Platform with Elliptic Curve Cryptography (ECC), the most widely used algorithms in use today in public and enterprise networks. As well as offering superior security, **SKA Platform endpoints agree keys 3.4x faster and are 2.5x more memory efficient than ECC.**