BUSINESS FINLAND

# Quantum-Safe Signing of Notification Messages Sent by Intelligent Transport Systems

**Authors** Sara Nikula

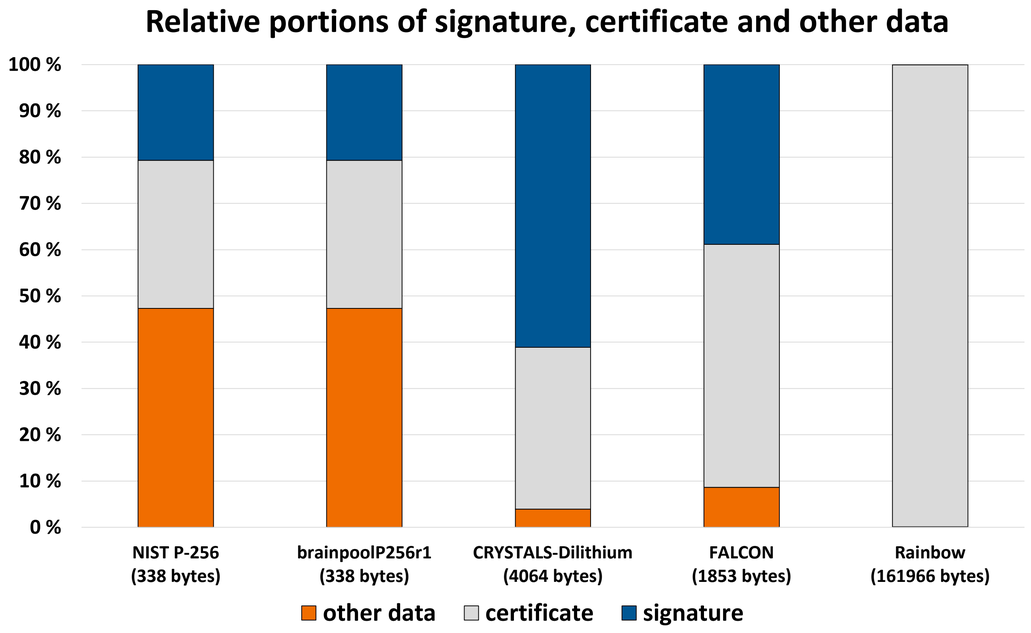
## C-ITS & PQC

Cooperative intelligent transport systems (C-ITS) improve safety and fluency in traffic by utilizing wireless communication. Digital signatures confirm origin and authenticity of these messages. According to the current technical specifications, published by European Telecommunications Standards Institute (ETSI), these digital signatures are created using elliptic curves. These signatures are at risk since they are based on elliptic curve discrete logarithm problem and thus they are not quantum-safe.

In this work, three quantum-safe digital signature algorithms, CRYSTALS-Dilithium, FALCON and Rainbow, were integrated into notification messages used by intelligent transport systems and specified in the standards published by ETSI. In our test program notification messages were signed using these quantum-safe digital signature algorithms and their suitability for this use was evaluated by measuring their speed in verification and signing and the size of the signed messages. These quantum-safe algorithms were also compared with the elliptic curves currently accepted by the standards.

## Results: message size

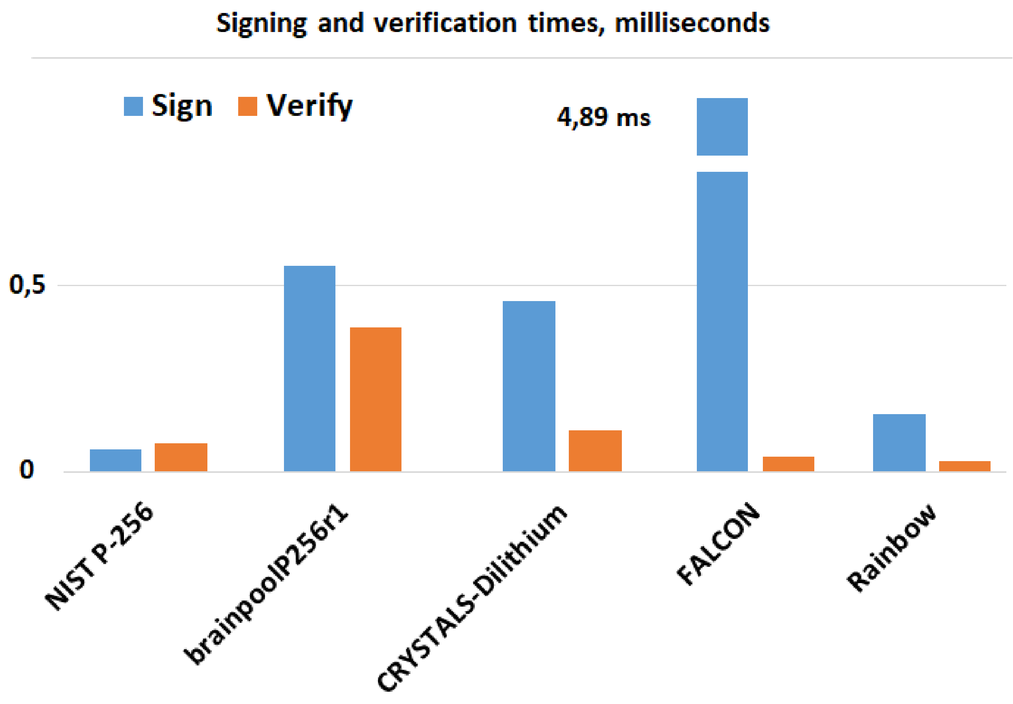
The size of the signed message is dependent on the size of the signature and the size of the public key, which are included in the signed message structure. All quantum-safe alternatives produce notably larger signed messages than elliptic curves (338 bytes). Multivariate-based Rainbow produces very large signed messages (161966 bytes) due to the size of its public key. Signed messages yielded by lattice-based FALCON and CRYSTALS-Dilithium are smaller (1853 and 4064 bytes).




Structures of the signed messages yielded by the different digital signature algorithms. Note that this chart represents the relative portions of different parts of the message. The total message sizes vary between these digital signature algorithms and are printed below the algorithm names.

## Results: signing and verification time

Our performance tests show that CRYSTALS-Dilithium, FALCON and Rainbow perform differently with regard to time required to sign and verify the sent messages. In the signing phase the variation in performance was notable, but in verification phase the quantum-safe alternatives were competitive. As a whole these quantum-safe digital signature algorithms perform quite well when compared to the elliptic curves currently accepted by the standard.




## The conclusions

Quantum-safe digital signatures could be used by intelligent transport systems with only moderate changes in performance. Based on these results, lattice-based alternatives are more suitable than multivariate-based. CRYSTALS-Dilithium is better portable between different processor architectures than FALCON.

This research was supported by PQC Finland project funded by Business Finland's Digital Trust program.

## Conclusion

- **In this work, quantum-safe digital signature algorithms were used to sign notification messages used by intelligent transport systems.**
- **Signing and verification times vary between different algorithms, as well as the size of the signed message.**
- **Based on the results, quantum-safe digital signatures could be used by intelligent transport systems with only moderate changes in performance. However message sizes will increase.**

**www.vttresearch.com**

**Contact:** Sara Nikula, Research Scientist
Tel. +358505344268, sara.nikula@vtt.fi

beyond the obvious