

# Post-quantum key exchange has shipped and the signatures have not

Every item is a hybrid key exchange. None is a post-quantum signature, so the certificates proving a website's identity are still classical. The algorithm changed at the dashed line, and the 2 sides are not compatible.

