Two of the 6 steps in a secure connection are the ones that break

The 6 steps of opening a secure connection. Two rely on mathematics a quantum computer can solve. The step that scrambles your actual content is not one of them, and no machine capable of either attack exists today.

1. Your device says which encryption methods it supports
2. The 2 sides agree on a shared secret over an open line **BREAKS**
3. The server proves who it is with a signed certificate **BREAKS**
4. The shared secret becomes a short-lived session key
5. Your content is scrambled with that session key **SURVIVES**
6. The connection closes and the session key is discarded

An eavesdropper records the whole connection, so breaking step 2 later recovers the session key and opens everything step 5 encrypted. Forward secrecy does not help, because the attack breaks the temporary key exchange itself.

Source: Shor, SIAM J. Computing 26(5), 1997; NIST IR 8105. LaMarr Labs, lamarrlabs.com/resources