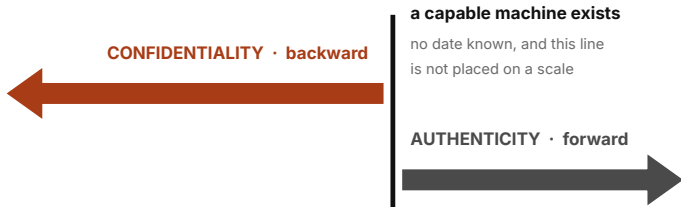


For confidentiality, the deadline is already here

Why quantum risk behaves unlike other security risks: for confidentiality the exposure is created years before anybody can act on it, so its deadline is today rather than whenever the machine arrives.



Backward.

Anything encrypted and recorded before that point, that still needs to stay secret afterwards, becomes readable. The exposure was created on the day the traffic was sent, so data you send today is already inside the sweep.

Forward.

Signatures and certificates can be forged from that point onward. Nothing signed before it is retroactively broken by the same attack.