Implementing Quantum-Resistant Cryptography in Industry

Samuel Sabogal Pardo

Should we be optimistic or pessimistic about the possibilities of quantum computing?

Current encryption techniques can be enhanced by wrapping old weak encryption content.

Quantum tech is getting near the point where RSA-2048 can be broken (372 Gbps).

In cybersecurity, we are not optimistic or pessimistic, we are all paranoid!

Asymmetric crypto

INFO → ⊕ → # → ⊕ → INFO

Public key

Private key

Symmetric crypto

INFO → ⊕ → # → ⊕ → INFO

Secret key

Secret key

Different physical properties allow quantum computers to have different kinds of algorithms.

I'm made from sand!

I'm made from gold!

We should be scared.

Quantum algorithm

\[ x = 0 \]

\[ -x = (1) \]