LMU LUDWIG-MAXIMILIANS-UNIVERSITÄT MÜNCHEN

MNM TEAM

Post-Quantum Key Exchange for IEEE 802.1AE

Antrittsvortrag zur Masterarbeit

Robin Lösch

loesch@cip.ifi.lmu.de

Aufgabensteller:	Prof. Dr. Dieter Kranzlmüller
Betreuer:	Tobias Guggemos
Betreuer:	Sophia Grundner-Culemann

September 2, 2020

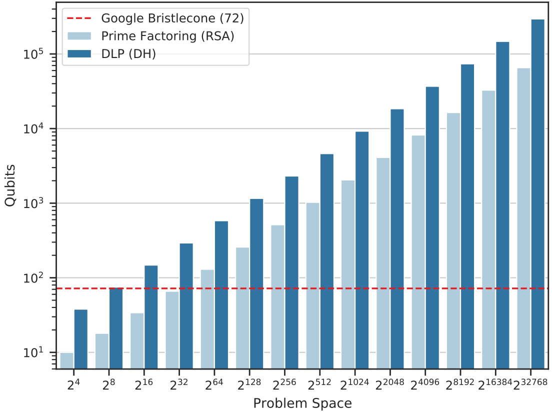
Practical Quantum Computer

When to panic?

Practical Quantum Computer

When to panic?

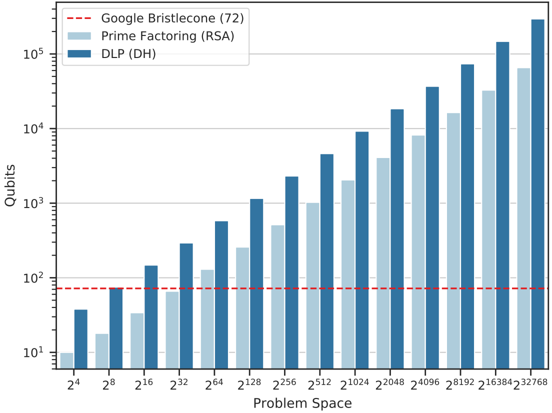
- #Qubits to break a n-bit key
  - RSA: $2n + 2$ [1]
  - DLP: $9n + 2\ln(n)$ [2]



Practical Quantum Computer

When to panic?

- #Qubits to break a n-bit key
  - RSA: $2n + 2$ [1]
  - DLP: $9n + 2\ln(n)$ [2]
- Coherency time
  - Keeping the state is tricky
  - Hard to predict
  - Strongly depends on technology



Practical Quantum Computer

- Even if we assume a Moore-like exp growth we still got plenty of time

Practical Quantum Computer

- Even if we assume a Moore-like exp growth we still got plenty of time
- We should use this time!

Practical Quantum Computer

- Even if we assume a Moore-like exp growth we still got plenty of time
- We should use this time!
    1. Design quantum safe crypto schemes

Practical Quantum Computer

- Even if we assume a Moore-like exp growth we still got plenty of time
- We should use this time!
  1. Design quantum safe crypto schemes
  2. **Implement quantum safe crypto schemes**