

PASQAL

QUANTUM DISCOVERY

Quantum speedup

PASQAL

www.pasqal.com

office@pasqal.com

7 rue Léonard de Vinci

91300 Massy

France

A first example

The problem of integer factorization

$$15 = 3 \times 5$$

A first example

The problem of integer factorization

711037990990982346997167372542447306435388248942717674118
 579730008893796655650496108364981484281589087722468
 943192090734451626219040776893338337738140787
 793199607009068946990324451757599047985
 309714010525845118363868937075102
 420531761340990920086193762
 330689198272181971464
 178555555157407
 303667618
 0046
 617-digit = 2048-bit RSA key
 438902256216469789162186128 = ? x ?

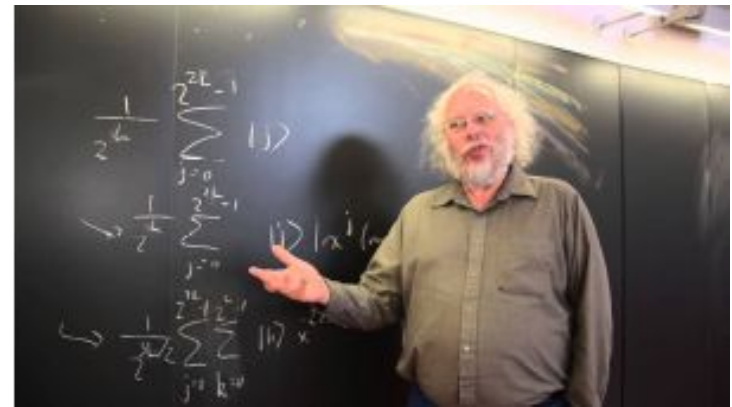
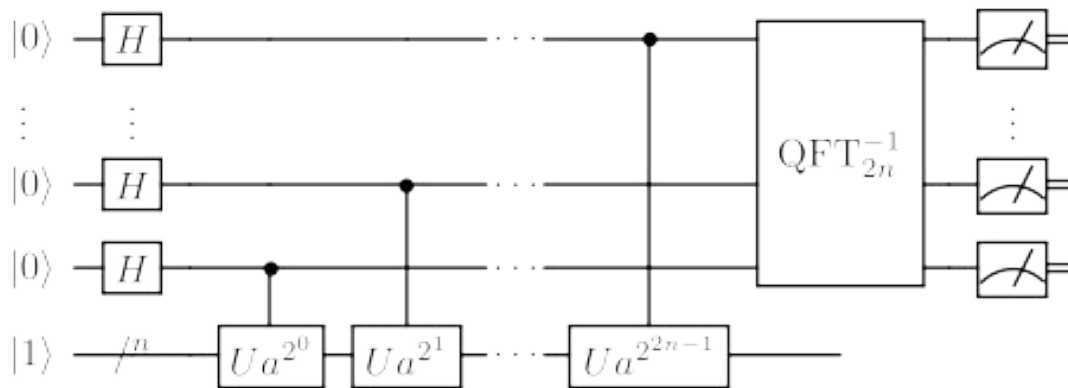
A first example

The problem of integer factorization

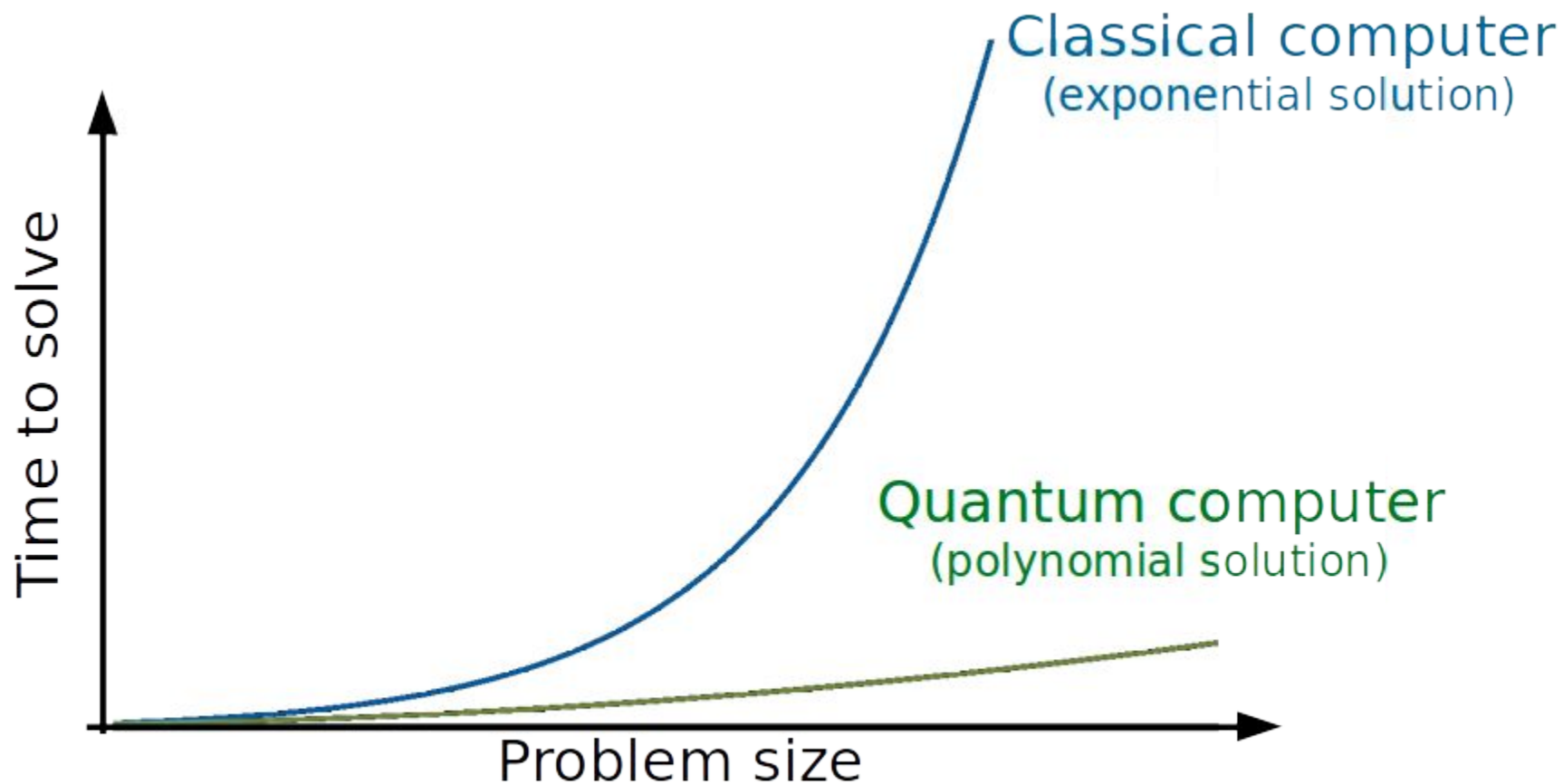
Finding the prime factors of a 2048-bit sequence:

- Classical computer (GHz clock rate): $\sim 10^{14}$ years
- Quantum computer (MHz clock rate, 4096 logical qubits): ~ 10 seconds

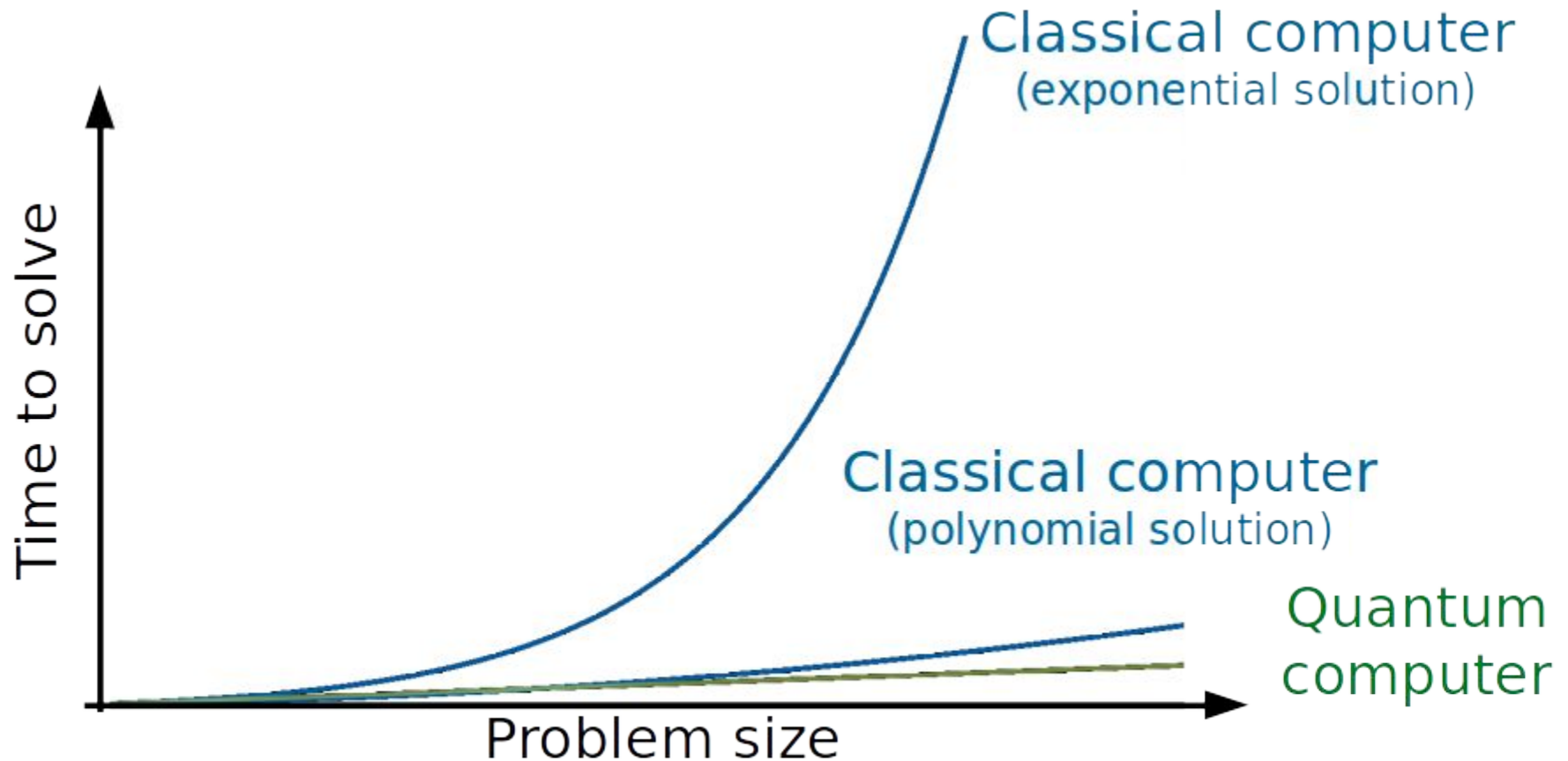
→ Shor's algorithm provides an **exponential speedup** !



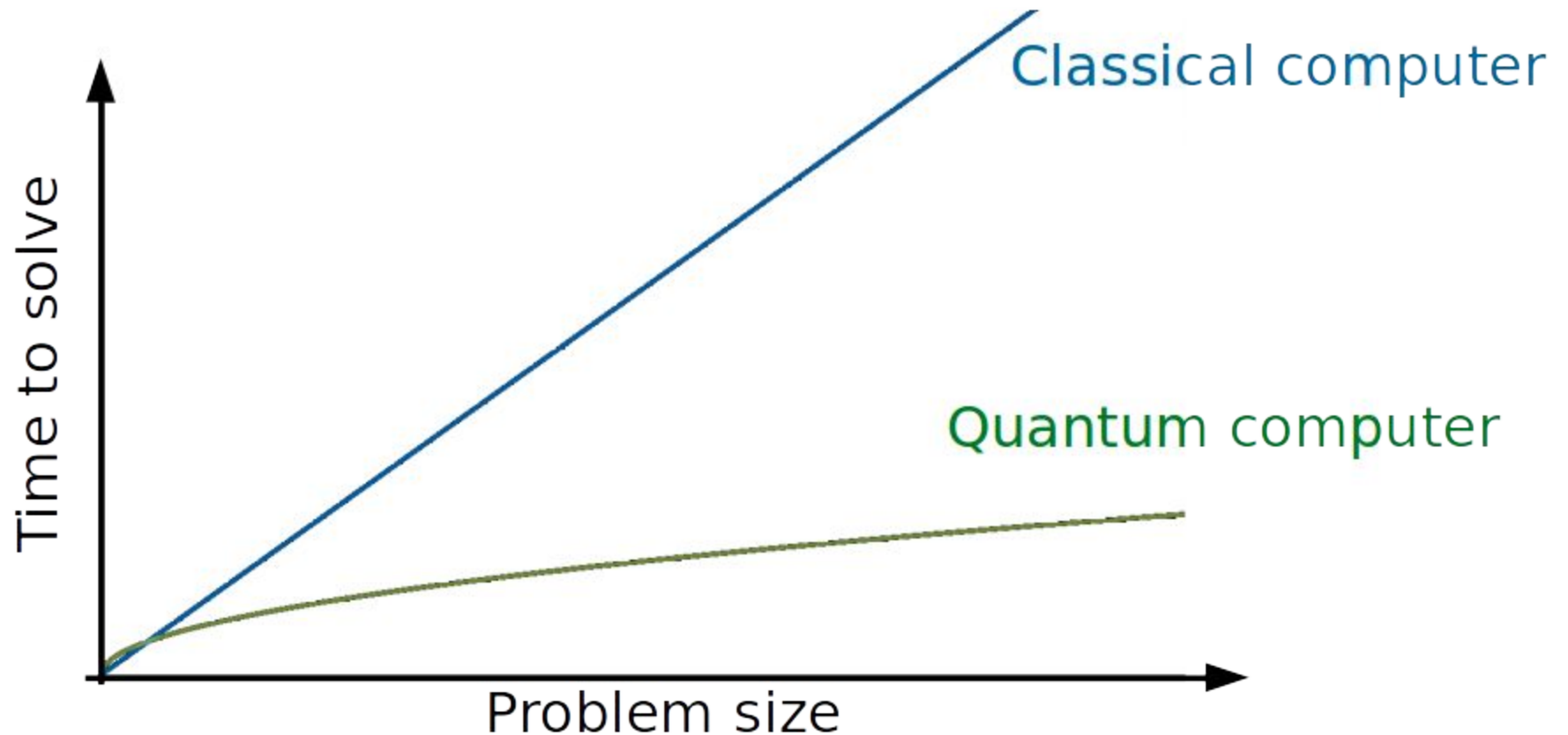
Exponential speedup



Quadratic speedup



Quadratic speedup



Conclusion

- Quantum computers will offer the possibility of performing certain computations much faster than classical devices
- Quantum speedup is the measure of this improved performance by quantum computers
- Some quantum algorithms provide an exponential speedup versus classical solutions, such as Shor's factoring algorithm
- While some other quantum algorithms provide a quadratic speedup, such as Grover's search algorithm
- A quadratic speedup is less significant than an exponential speedup
- The case of hybrid quantum-classical algorithms will be discussed in next videos as there is no clear view on their algorithmic complexity