Quantum Computing
and
Quantum Cryptography

Thierry Sans

Quantum Computing

A quantum computer uses **quantum bits** and relies on of **quantum-mechanical phenomena** to perform computation

1. Brute-forcing n-bits key with <u>Grover's algorithm</u> would take **$2^{n/2}$**
   ➡ Using symmetric encryption is still doable

2. Factoring prime numbers with <u>Shor's algorithm</u> would be done in polynomial time
   ➡ Using asymmetric encryption is at risk
   ➡ Problem for key exchange