

The background features a light gray grid pattern overlaid with a vibrant, abstract splash of colors. The colors transition from warm oranges and reds on the left to cool blues and greens on the right, with a purple hue in the center. The splatters vary in size, creating a dynamic and artistic effect.

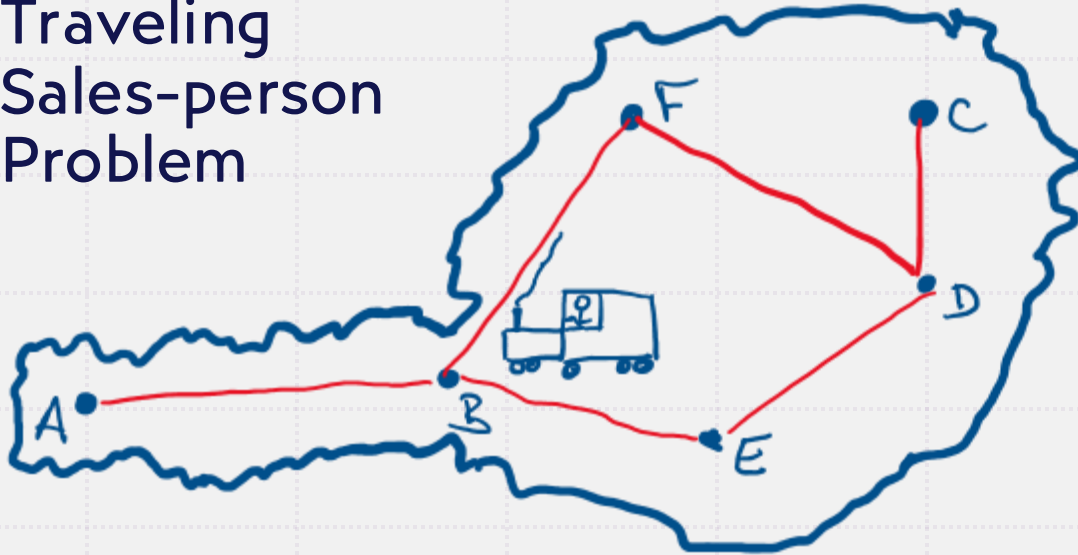
Julia Freund

Institut für Theoretische Physik (Universität Innsbruck)

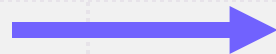
# Principles and Applications of Quantum Information

# Motivation

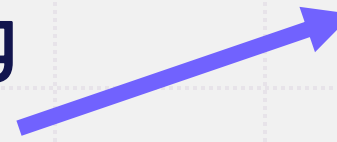
Traveling  
Sales-person  
Problem



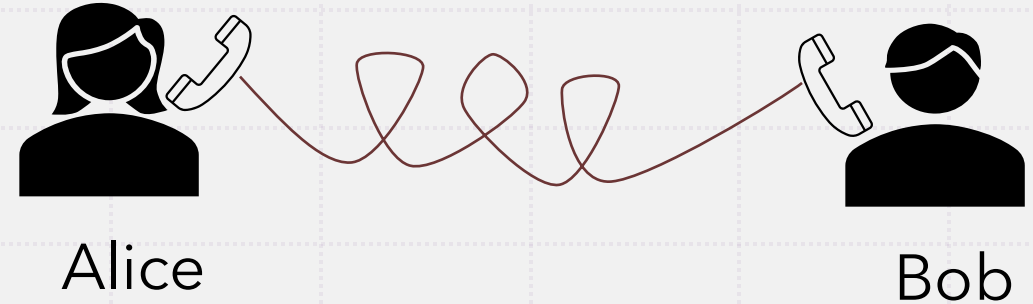
Can a quantum  
computer solve NP-  
hard problems faster  
than a classical  
computer?



Factoring  
Problem  
(RSA)

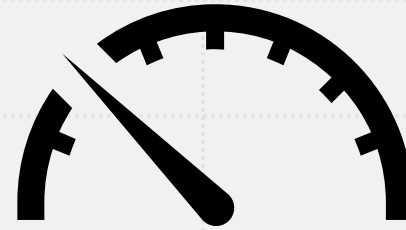
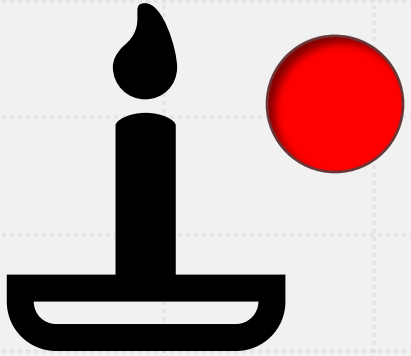


Secure communication  
Key exchange



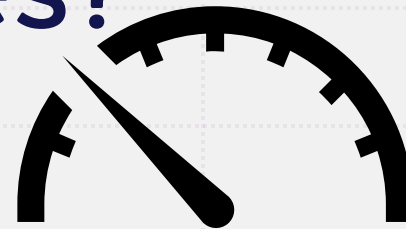
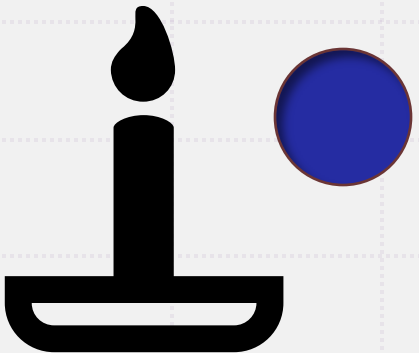
How can we use  
quantum particles to  
exchange a key  
between Alice & Bob?

# Classical Light Source



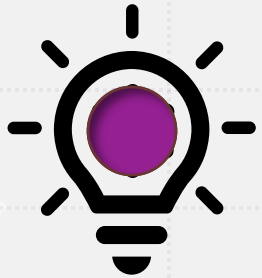
red  
100%

What makes quantum particles different from classical particles?

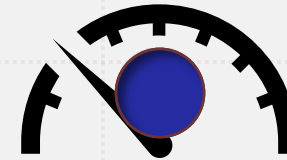


blue  
100%

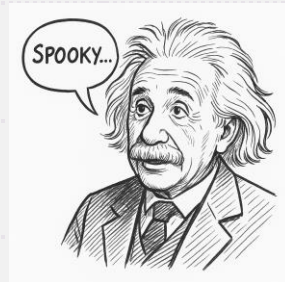
# Quantum Light Source



Superposition



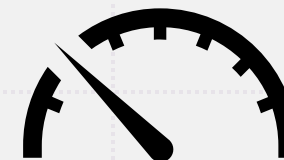
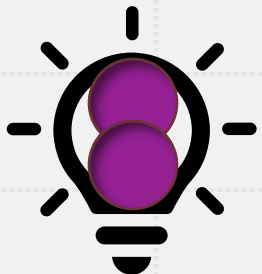
red  
50%  
blue  
50%



Entanglement



red  
50%  
blue  
50%



red  
100%

# Definition of a quantum bit

$|0\rangle = \text{red circle} = \text{"0" bit}$

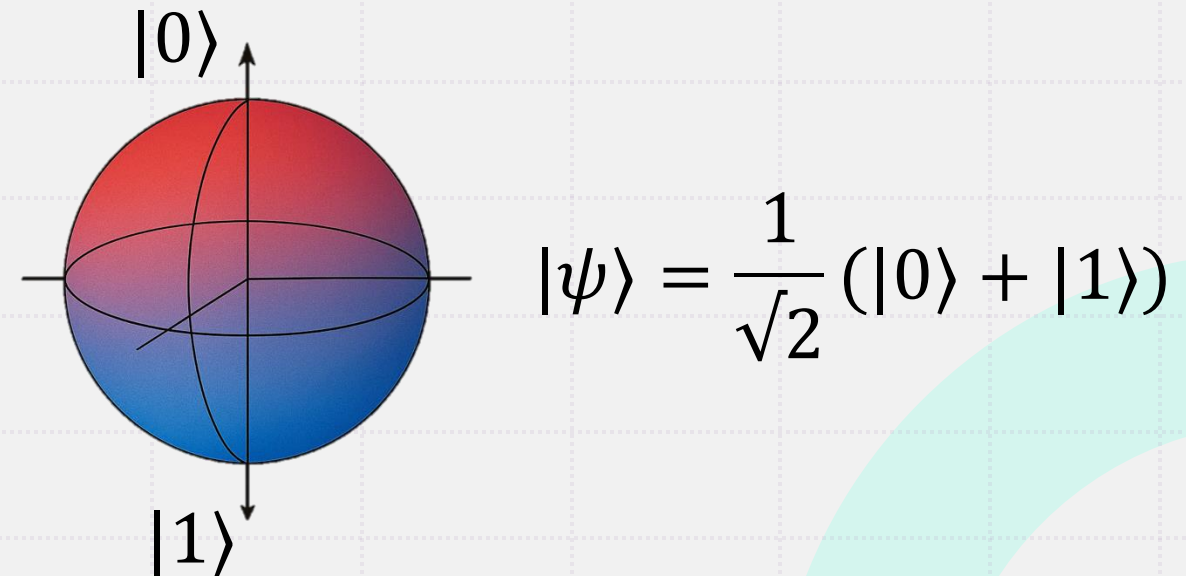
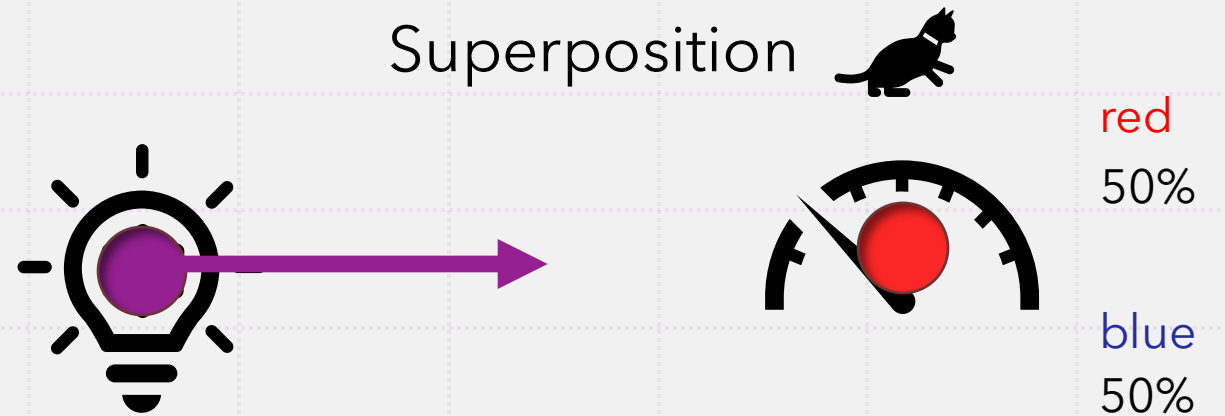
$|1\rangle = \text{blue circle} = \text{"1" bit}$

Quantum bit - qubit:

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$$

$\alpha$  ~ probability that we find 0 (red)

$\beta$  ~ probability that we find 1 (blue)



# Deutsch-Josza Algorithm (1)

Task: determine if function  $f$  is **constant** or **balanced**

Boolean function:  $f: \{0,1\} \mapsto \{0,1\}$

$f_1: 0 \mapsto 0$   
 $1 \mapsto 0$   
 $f_2: 0 \mapsto 1$   
 $1 \mapsto 1$

} **constant**

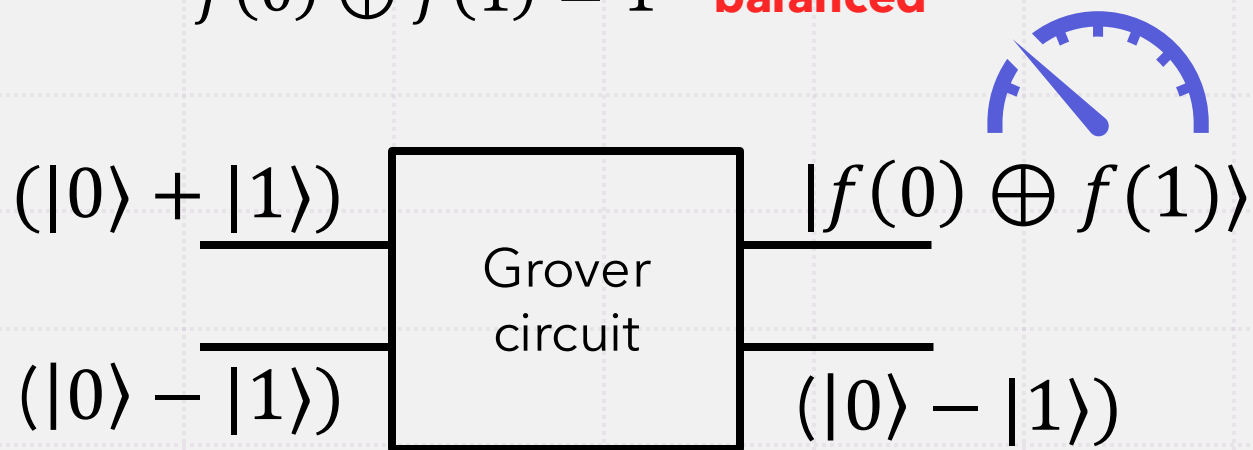
$f_3: 0 \mapsto 0$   
 $1 \mapsto 1$   
 $f_4: 0 \mapsto 1$   
 $1 \mapsto 0$

} **balanced**

Quantum strategy:

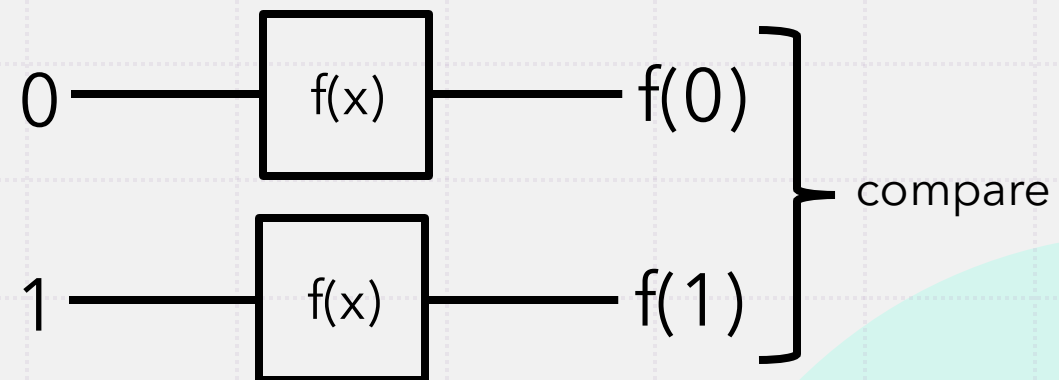
$$f(0) \oplus f(1) = 0 \quad \text{constant}$$

$$f(0) \oplus f(1) = 1 \quad \text{balanced}$$



1 step

Classical strategy:



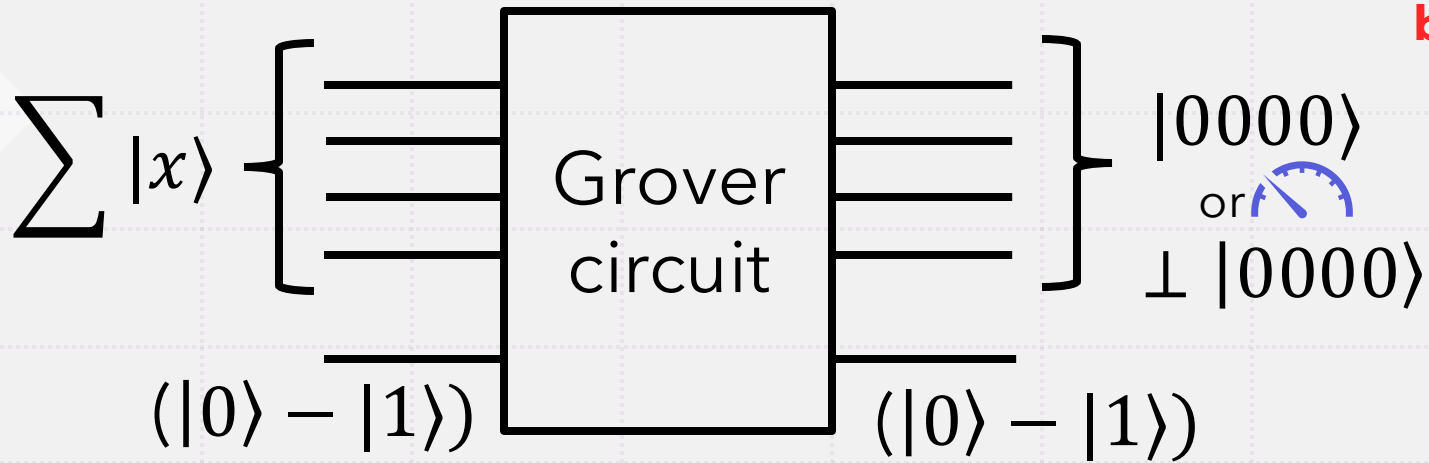
2 steps

# Deutsch-Josza Algorithm (2)

Generalization to m bit function:  $f: \{0,1\}^m \mapsto \{0,1\}$

Promise:  $f(x) = \text{const.} \forall x \in \{0,1\}^m$  **constant**

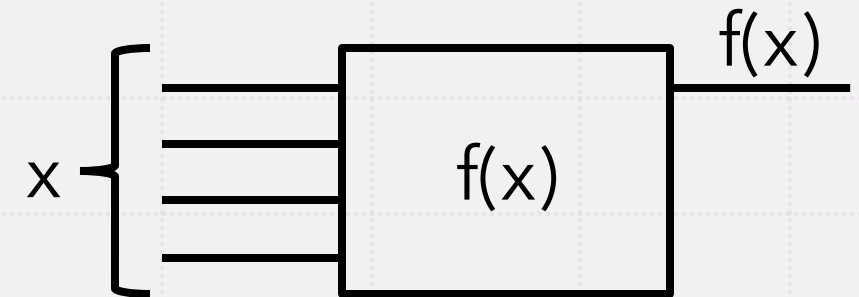
Quantum strategy:



$$f(x) = \begin{cases} 0, & \forall x \in M_0 \\ 1, & \forall x \in M_1 \end{cases} \text{ with } \begin{cases} M_0 \cup M_1 = \{0,1\}^m \\ M_0 \cap M_1 = \emptyset \\ |M_0| = |M_1| = 2^{m-1} \end{cases}$$

**balanced**

Classical strategy:



$|0000\rangle$  **constant**

Something else, e.g.:  
 $|0010\rangle$

**balanced**

1 step

$2^{m-1} + 1$

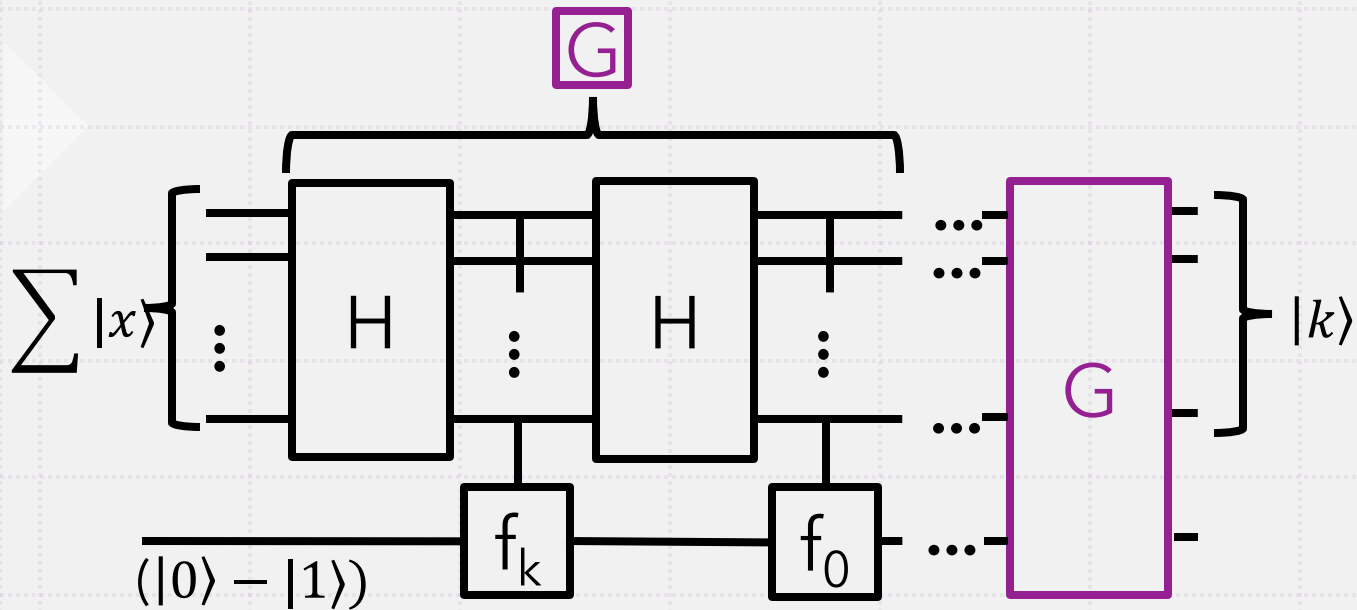
steps/repetitions

(in the worst case to be 100% sure about it)

# Other Algorithms

Grover's Algorithm:  $f: \{0,1\}^m \mapsto \{0,1\}$

$$f(x) = \begin{cases} 1, & x = k \\ 0, & x \neq k \end{cases} \quad N = 2^m \text{ Numbers/ Bit patterns}$$



Classically:  $\mathcal{O}(N)$

Quantum:  $\mathcal{O}(\sqrt{N})$  times we apply **G**

with probability  $p = 1 - 1/\sqrt{N}$

Shor's Algorithm:

Prime number factorization

$$N = p \cdot q \quad N \text{ is a } m \text{ bit number}$$

Task: find  $p$  and  $q$

Classical:  $\mathcal{O}(\sqrt{N})$  Exponential in  $N$


Quantum:

$$\mathcal{O}((\log N)^2) \rightarrow \mathcal{O}(m^2)$$

Exponential in number of bits  $m$




# Quantum Key Distribution

 = 101011101001 (random sequence of 0, 1)



Alice

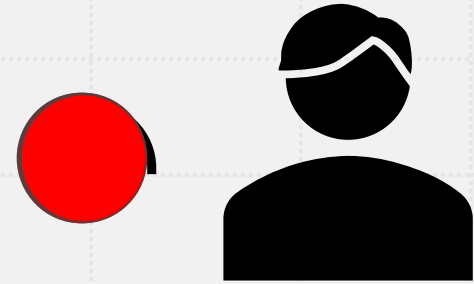


 = 101011...




Repeat that many times

Eavesdropper detection



Bob



 = 101011...

# Teleportation

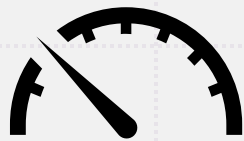
Alice has a qubit in the state:  $|\Psi\rangle$

Task: get Bob the state

Alice and Bob share an **entangled state**

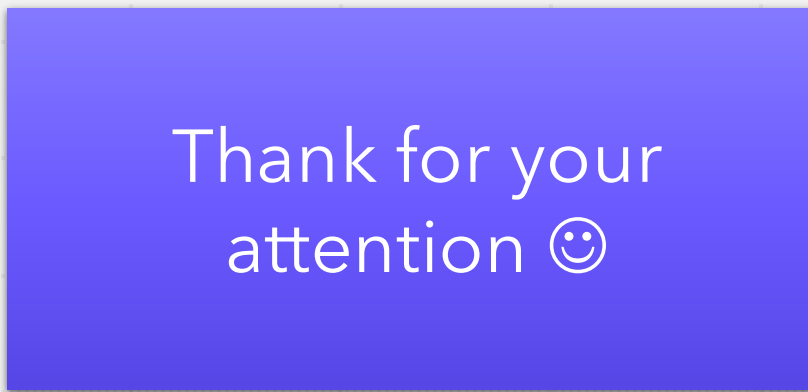


Alice

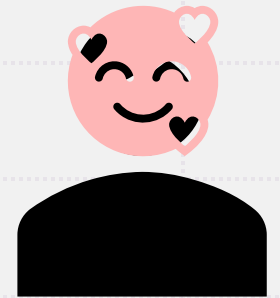
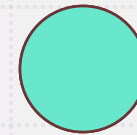


Bell measurement

Gets outcome  $i$  out of four



Alice tells Bob  $i$



Bob

$$U_i |\Psi\rangle$$

$$U_i^\dagger U_i |\Psi\rangle = |\Psi\rangle$$

Bob applies the inverse to his qubit