

# The quest for secure quantum communication



Ramona Wolf, University of Siegen

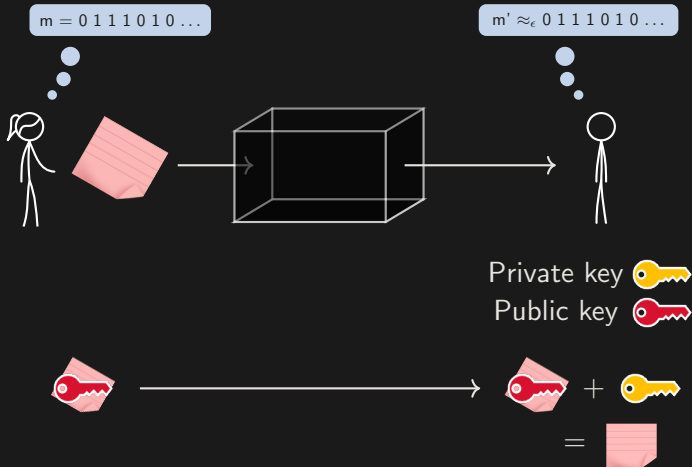


**Why do we need quantum cryptography?**



# A glimpse of classical cryptography

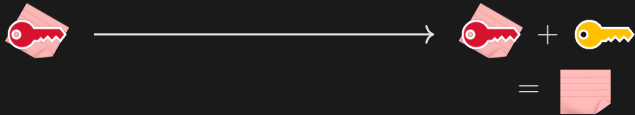
*RSA encryption*



Is this secure?




# What makes RSA secure?



Public key:  =  $p \cdot q$

$p, q$  randomly chosen, large prime numbers

Knowledge of  $p, q \Rightarrow$  Can calculate the private key 

Why is this secure?

$\Rightarrow$  Factoring large numbers is hard

Not for a quantum computer!

# General problems in classical cryptography

We do not know if  
there exists an algorithm  
that breaks the encryption  
(classical or quantum)  
— encryption can be  
broken anytime



“Store now, decrypt later”  
attacks make quantum  
computers already  
a security  
threat today



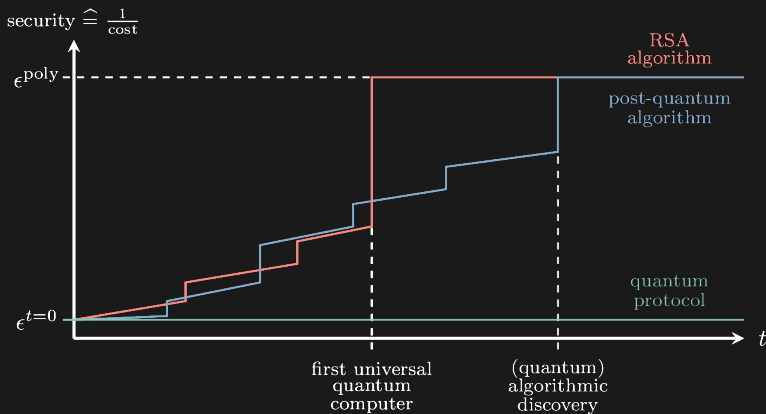
Computational  
power (classical  
or quantum)  
increases over  
time

Table I.

Digits	Number of operations	Time
50	$1.4 \times 10^{10}$	3.9 hours
75	$9.0 \times 10^{12}$	104 days
100	$2.3 \times 10^{15}$	74 years
200	$1.2 \times 10^{23}$	$3.8 \times 10^6$ years
300	$1.5 \times 10^{29}$	$4.9 \times 10^{15}$ years
500	$1.3 \times 10^{39}$	$4.2 \times 10^{25}$ years

# Security over time

*Classical vs. quantum protocols*



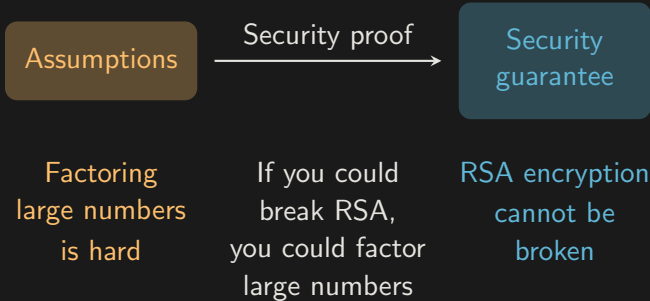
What makes quantum crypto secure?





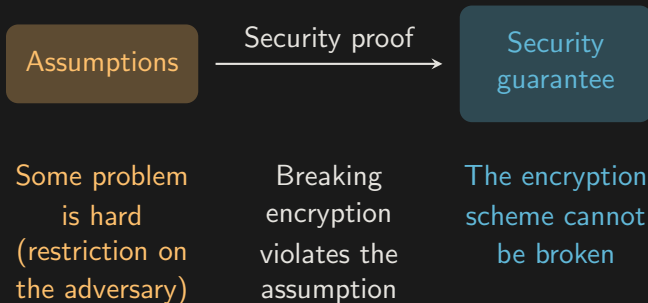
# Security proofs in cryptography

*Classical cryptography*



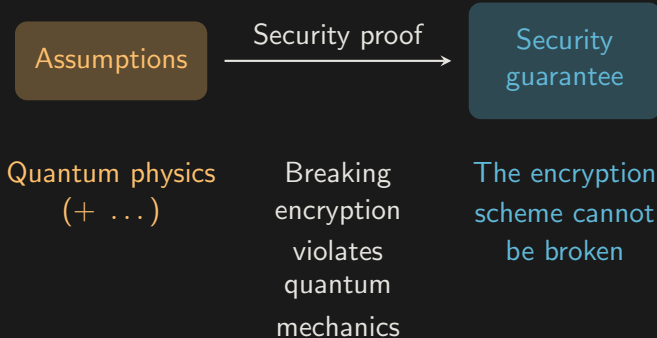
# Security proofs in cryptography

*Classical cryptography*



# Security proofs in cryptography

*Quantum cryptography*

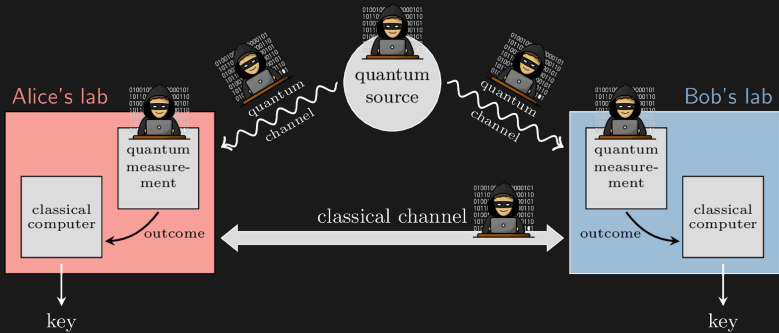


# How does QKD work?



# QKD protocol

*The setup*



# QKD protocol

## *Steps*

Quantum phase:

1. For  $n$  rounds: Quantum states are distributed to Alice and Bob
2. Alice and Bob measure the states
3. Alice and Bob have raw keys  $A_1, \dots, A_n$  and  $B_1, \dots, B_n$

Classical post-processing:

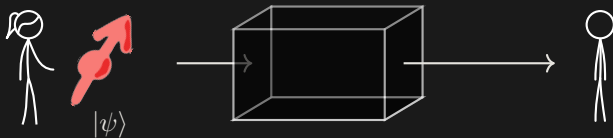
4. Alice and Bob estimate the knowledge of a possible eavesdropper (via Bell violation, errors in the bit strings,...)

Important quantity:  $H_{\min}^{\epsilon}(A_1, \dots, A_n|E)$

5. Error correction: Turn raw keys into identical bit strings
6. Privacy amplification: Remove the adversary's knowledge

# QKD protocol

*Why does this work?*



# QKD protocol

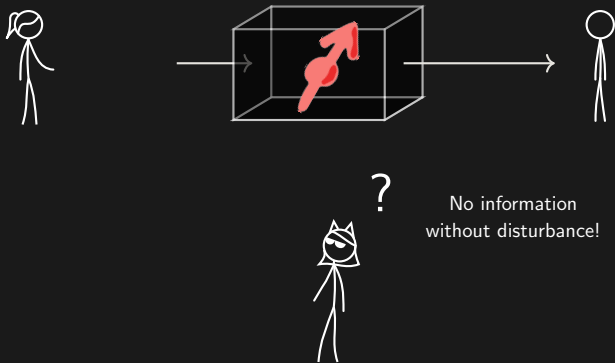
*Why does this work?*





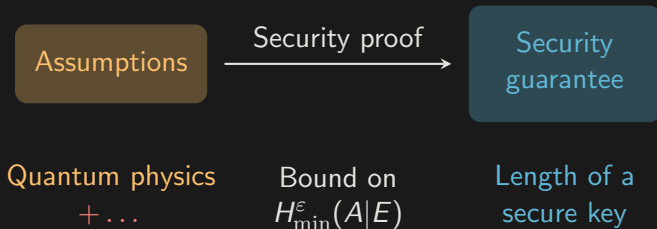
# QKD protocol

*Why does this work?*



# Security proofs in cryptography

*Quantum cryptography*

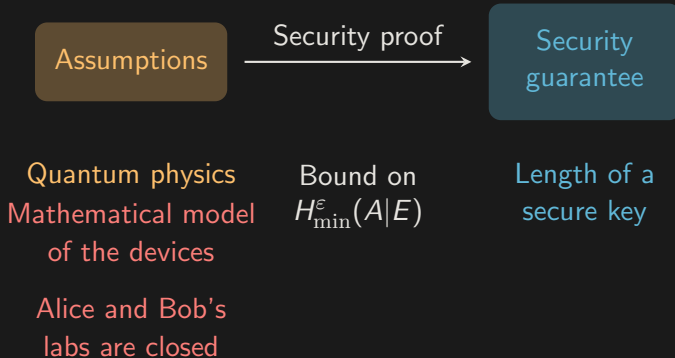


**We need to talk about assumptions**



# Assumptions on QKD

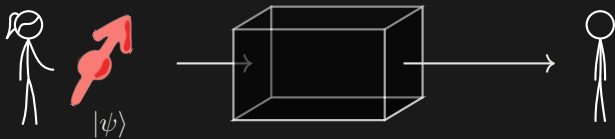
*What do we trust?*



**What is information?**



# What is information?

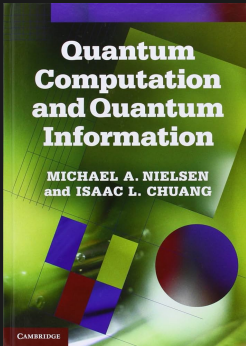


*"Information is Physical"*

- R. Landauer

# Quantum information theory

*Nielsen-Chuang*



P1: Isolated system  $S \rightarrow$  Hilbert space  $\mathcal{H}$

P2: State of  $S \rightarrow$  norm-1 vector  $\psi \in \mathcal{H}$

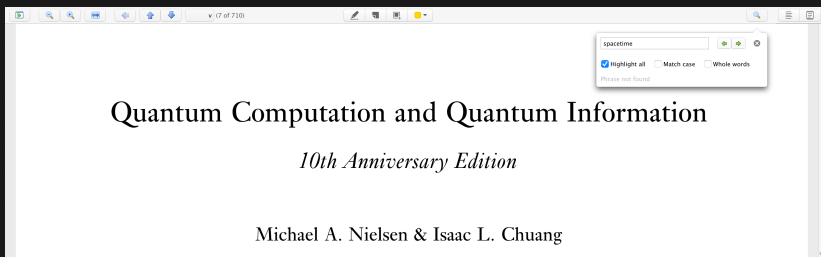
P3: Isolated evolution  $\rightarrow$  unitary  $\psi_2 = U\psi_1$

P4: Meas.  $\rightarrow P(m) = \langle \psi | M_m^\dagger M_m | \psi \rangle$

$$\psi_m = \frac{M_m |\psi\rangle}{\sqrt{P(m)}}$$

# Spacetime in QIT

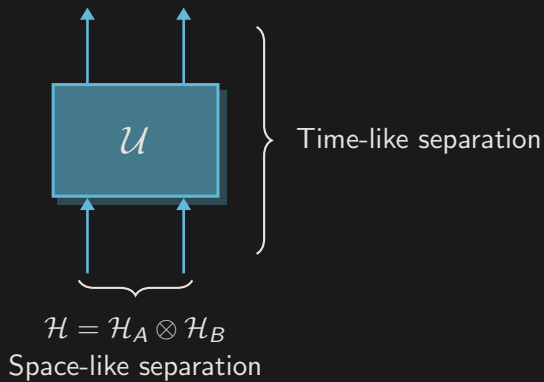
*Nielsen-Chuang*





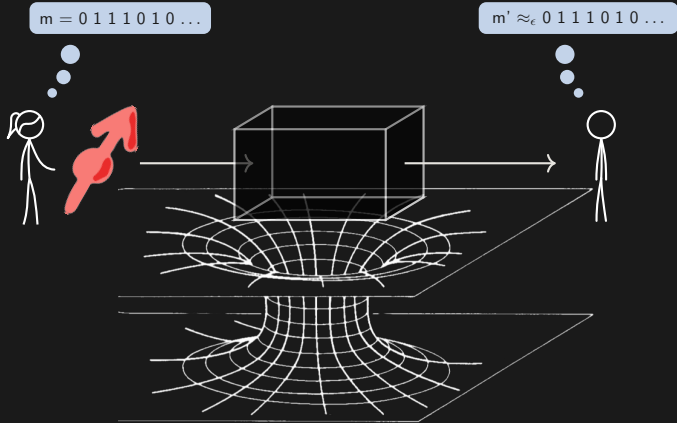
# Spacetime in QIT

(abstracted to a simple partial order notion)



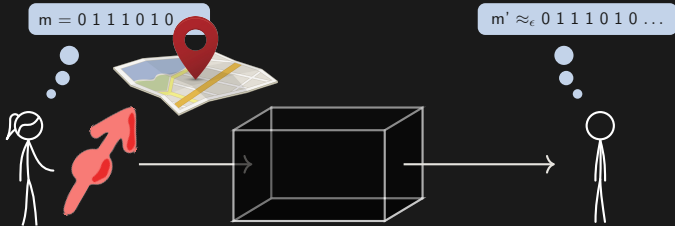
# Spacetime in QIT

(abstracted to a simple partial order notion)



# Spacetime in QIT

(abstracted to a simple partial order notion)



“Information is physical”

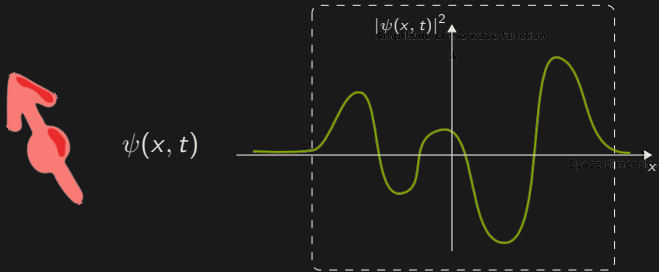
Physical systems occupy a region of spacetime

→ Information occupies a region of spacetime

**Where is information localised?**



## Location of particles



For any  $t$ , it's the smallest region  
where the particle is found with certainty

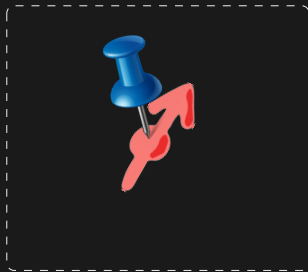
## Location of information?

## Locating a bit encoded in one particle

$$|\psi\rangle = \frac{1}{\sqrt{2}} (|0\rangle \boxed{\pm} |1\rangle)$$



— enc —→



Location: same as particle 1

## Locating a bit encoded in two particles

$$|\psi\rangle = \frac{1}{\sqrt{2}} (|01\rangle \boxed{\pm} |10\rangle)$$



Location: same as particles 1 and 2

## Locating a bit encoded in two particles

$$|\psi\rangle = \frac{1}{\sqrt{2}} (|01\rangle \boxed{\pm} |10\rangle)$$



What if we can only access relative degrees of freedom?



## Quantum reference frames (QRF)

If QM is universally valid, systems that are used as a reference are ultimately quantum mechanical

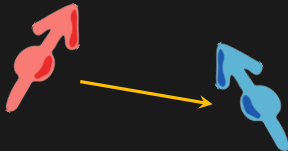


# Quantum reference frames (QRF)

If QM is universally valid, systems that are used as a reference are ultimately quantum mechanical

Taking the perspective of 1:

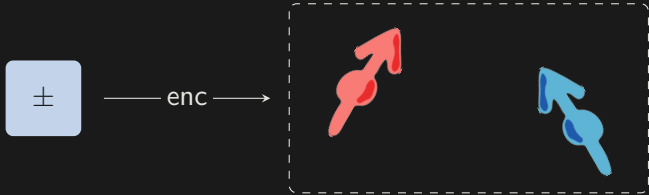
$$|x_1\rangle_1 |x_2\rangle_2 \mapsto |x_2 - x_1\rangle_{2|1}$$



# Locating a bit encoded in two particles

Taking the perspective of 1

$$|\psi\rangle = \frac{1}{\sqrt{2}} (|10\rangle \boxed{\pm} |01\rangle)$$

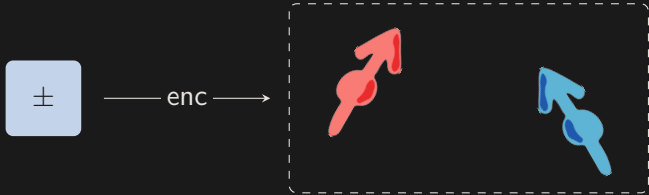


Location: same as particles 1 and 2

# Locating a bit encoded in two particles

Taking the perspective of 1

$$|\psi\rangle_{2|1} = \frac{1}{\sqrt{2}} (|1\rangle \boxed{\pm} | - 1\rangle)$$

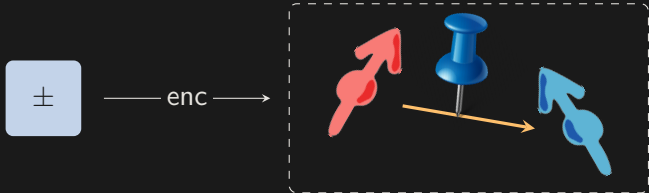


Location: same as particles 1 and 2

# Locating a bit encoded in two particles

Taking the perspective of 1

$$|\psi\rangle_{2|1} = \frac{1}{\sqrt{2}} (|1\rangle \boxed{\pm} | - 1\rangle)$$



Location: same as particles 1 and 2 (specifically in the relative dof)

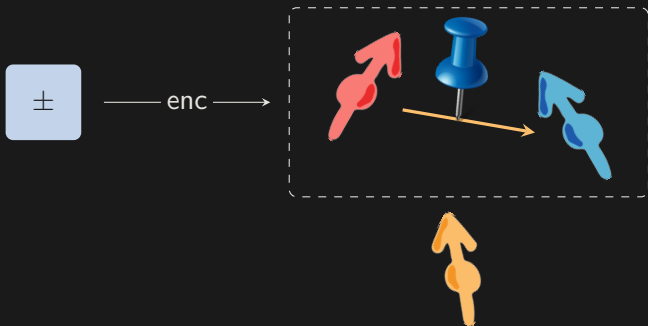
# Locating a bit encoded in three particles

$$|\psi\rangle_{123} = \frac{1}{\sqrt{2}} (|01\rangle \boxed{\pm} |10\rangle) |0\rangle$$



# Locating a bit encoded in three particles

$$|\psi\rangle_{123} = \frac{1}{\sqrt{2}} (|01\rangle \boxed{\pm} |10\rangle) |0\rangle$$

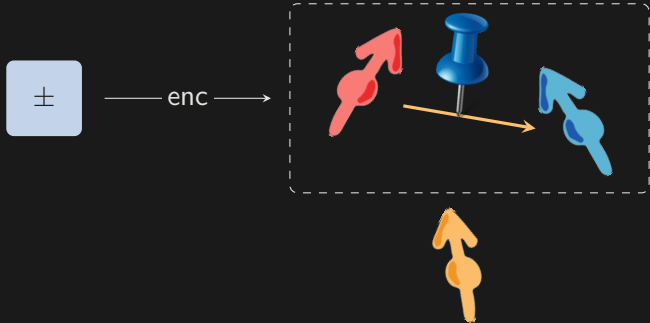


Location: same as particles 1 and 2 (specifically in the relative dof)

# Locating a bit encoded in three particles

Taking the perspective of 1

$$|\psi\rangle_{23|1} = \frac{1}{\sqrt{2}} (|10\rangle \boxed{\pm} | -1 -1\rangle)$$



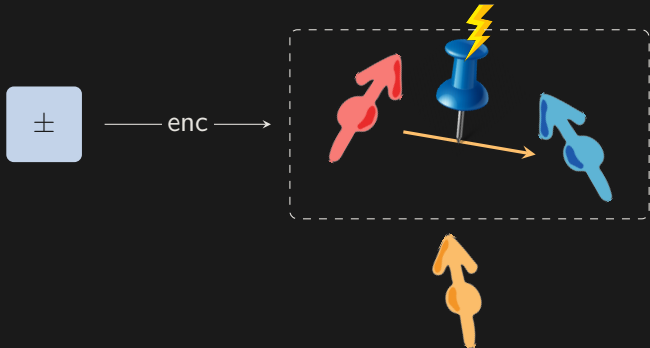
Location: same as particles 1 and 2 (specifically in the relative dof)



# Locating a bit encoded in three particles

Taking the perspective of 1

$$|\psi\rangle_{23|1} = \frac{1}{\sqrt{2}} (|10\rangle \boxed{\pm} | - 1 - 1\rangle)$$



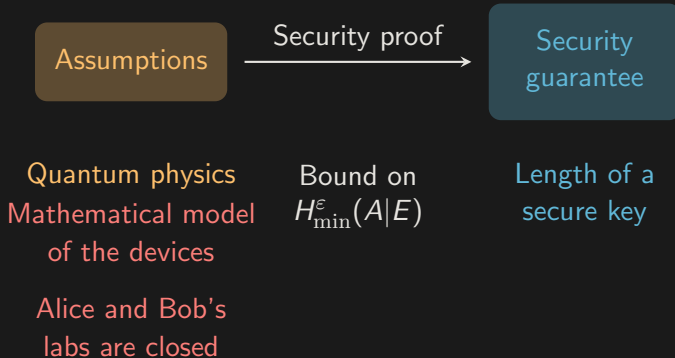
Frame-dependent location?

## Implications for cryptography

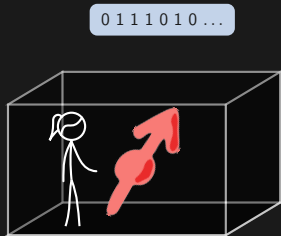


# Assumptions on QKD

*What do we trust?*

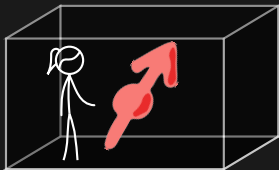


## Closed lab assumption

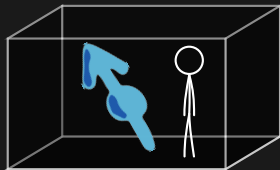


## Closed lab assumption

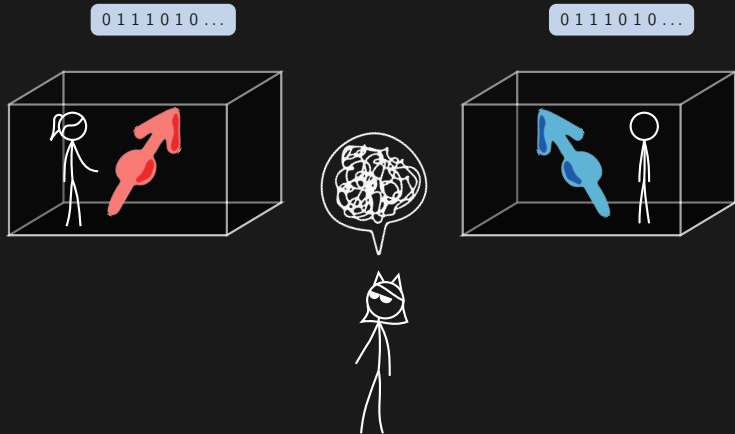
0111010...



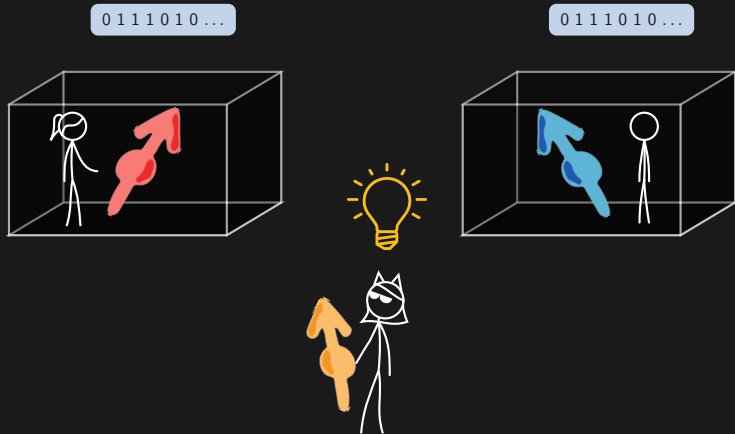
0111010...



## Closed lab assumption



## Closed lab assumption



# Conclusion





# Conclusion

Assuming the universality of quantum mechanics, information is not objectively localised.

→ How does this affect cryptography?

Look for concrete attacks that would exploit features of quantum reference frames and adapt security.

→ More general: Assumptions in QKD

How can we bring the theoretical models and practical implementations closer together? What are reasonable assumptions?

