Trento 29/10/2025

Tensors in Quantum Cryptography

Claudia De Lazzari - PhD

Who I am

- Bachelor and Master degree in Mathematics – University of Padova
- PhD in Mathematics – University of Trento + Q@TN
  - Alessandra Bernardi
  - Iacopo Carusotto
- Quantum Cryptographer – QTI s.r.l., Firenze

Summer 2019

Spring 2022

Autumn 2025

QTI – Quantum Telecommunications Italy

QTI is a company **founded in October 2020** as a spin-off of the Italian National Institute of Optics of the National Research Council (CNR).

First Italian **Quantum Key Distribution (QKD)** company, design, development and production of industrial grade systems for quantum networks.

2020
QTI is founded as spin-off of CNR-INO

2021
Telsy (TIM Group) invests in QTI company share

2022
Telsy increases its share reaching 49%

2024
Telsy increases its share reaching 80%

Today
QTI is a Telsy's subsidiary company

35 people
90% Technical Staff
84% under 37

Summary

- Why Quantum Key Distribution (QKD)
- Prepare and Measure BB84 protocol (Bennet, Brasserd 1984)
  - Description
  - Sketch of tensorial formalism
  - Eavesdropper action

Why QKD?

Key Distribution

GOAL : distribution of a **secure** key between parties:for encryption/decription

Key Distribution

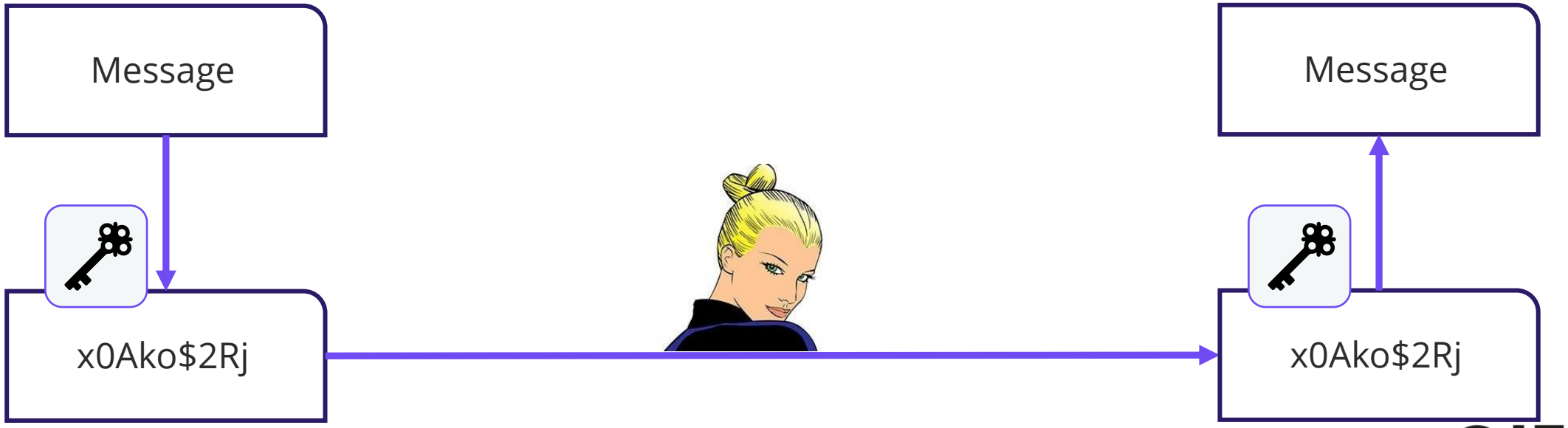
GOAL : distribution of a **secure** key between parties:for encryption/decription

Message

Message

Key Distribution

GOAL : distribution of a **secure** key between parties:for encryption/decription



Quantum Key Distribution

GOAL : distribution of a key between parties **inconditionally** secure

All attacks, admitted by the laws of QM

Quantum Key Distribution

GOAL : distribution of a key between parties: **inconditionally** secure

All attacks, admitted by the laws of QM

Conventional key distribution

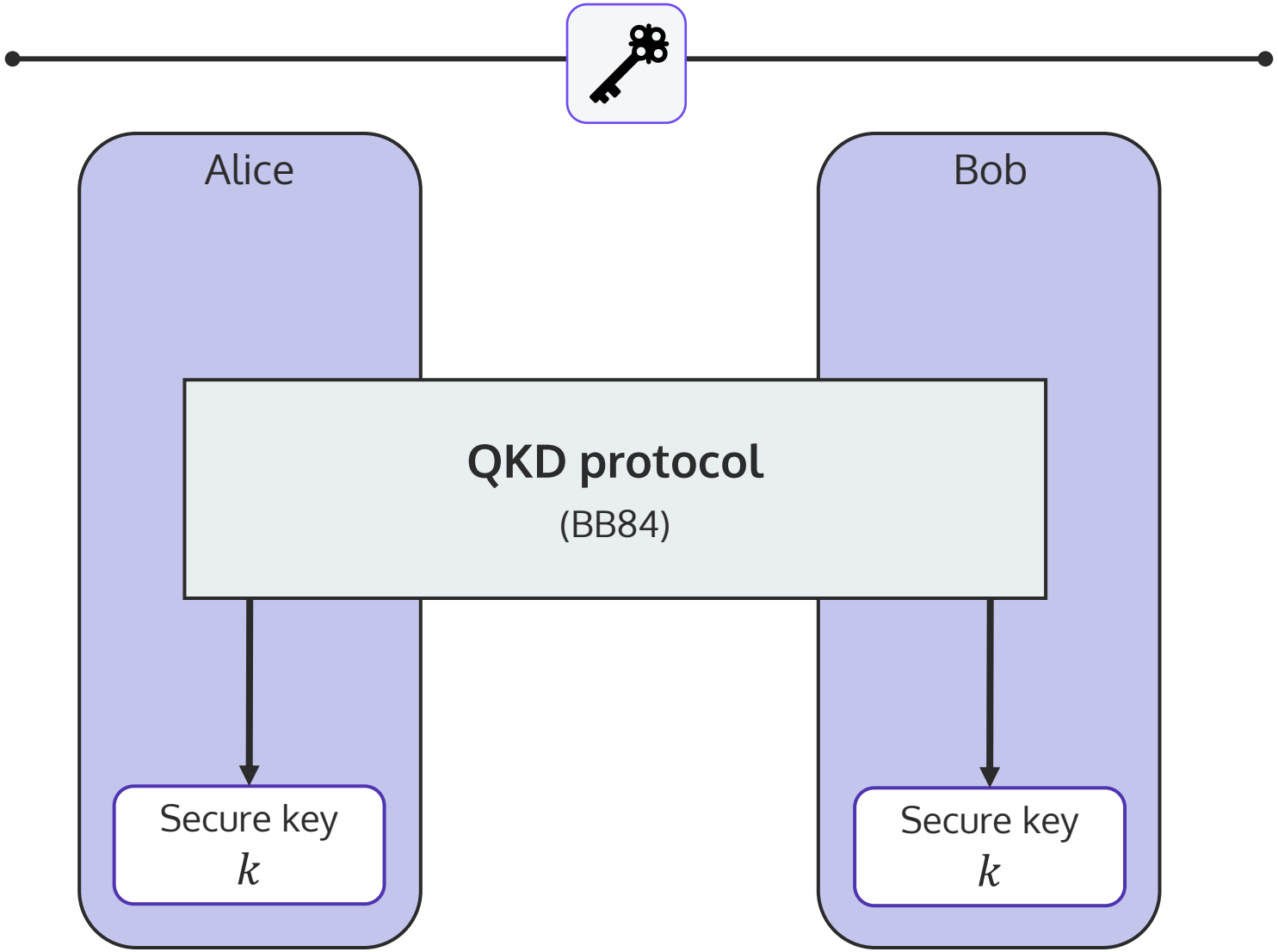
- Security relies on **hardness assumption**
- **Assumptions** on available technologies (computational power)
- **No** future-proof security

Quantum key distribution

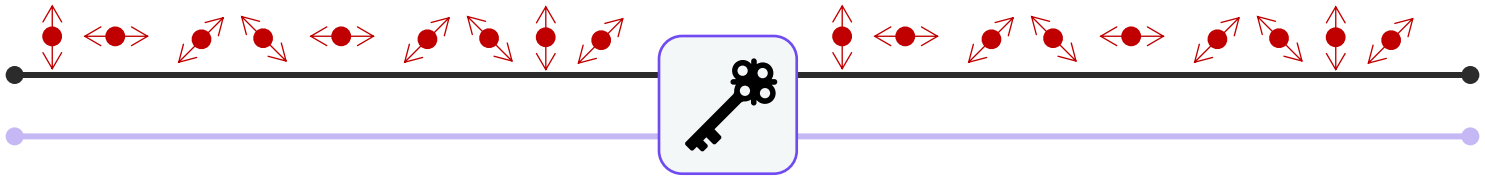
- **Security** mathematically quantified from physical laws
- No need to make **assumptions** on the enemy's resources
- **Future-proof** security

Prepare and Measure BB84

Quantum Key Distribution protocol



Quantum Channel



Alice

Bob

Quantum communication

Prep. and meas. of quantum states,
distributed in the quantum channel

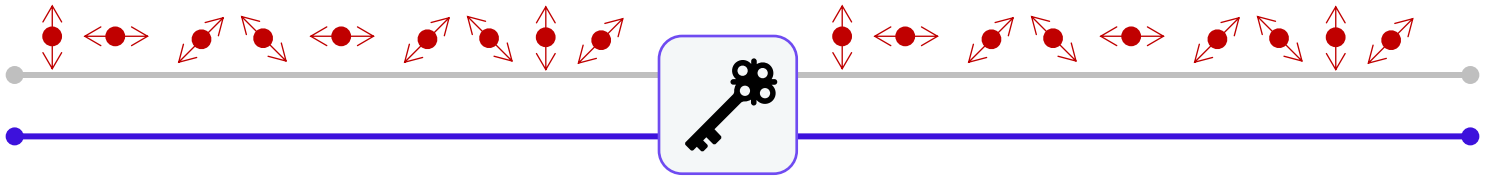
Classical post-processing

Elaboration of quantum results
via public discussion in the classical channel
(short-term authentication)

Secure key
k

Secure key
k

Classical Channel



Alice

Bob

Quantum communication

Prep. and meas. of quantum states,
distributed in the quantum channel

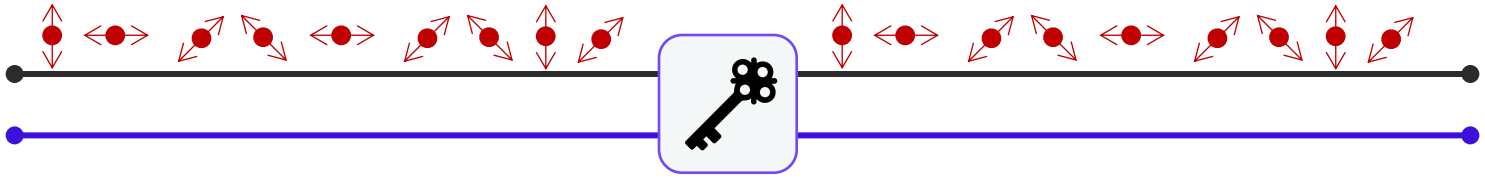
Classical post-processing

Elaboration of quantum results
via public discussion in the classical channel
(short-term authentication)

Secure key
k

Secure key
k

QKD Protocol



Alice

Bob

Quantum communication

Prep. and meas. of quantum states,
distributed in the quantum channel

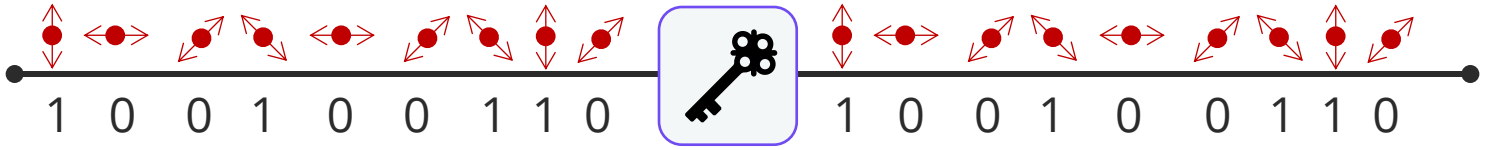
Classical post-processing

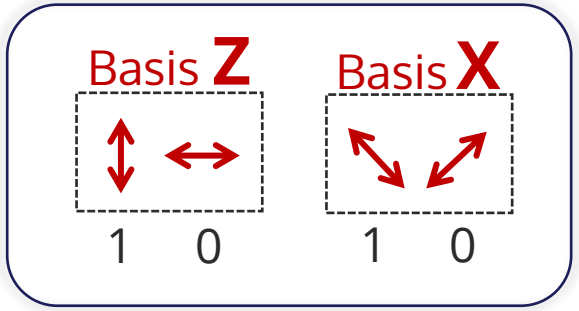
Elaboration of quantum results
via public discussion in the classical channel
(short-term authentication)

Secure key
k

Secure key
k

Quantum communication

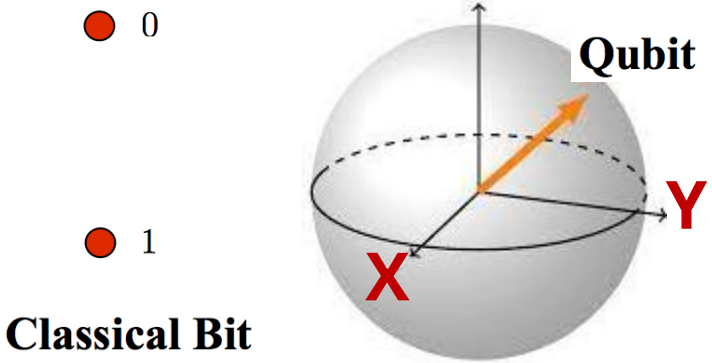




Quantum Superposition

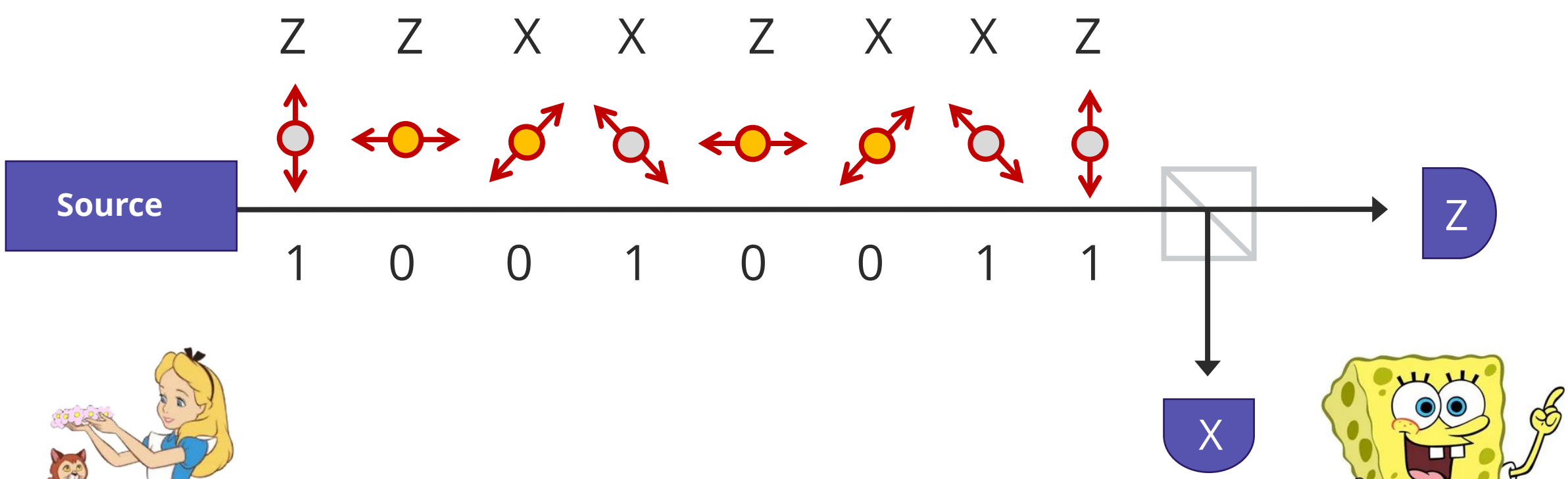
$$\leftrightarrow = \frac{\leftrightarrow + \updownarrow}{\sqrt{2}}$$

$$\nwarrow\!\!\searrow = \frac{\leftrightarrow - \updownarrow}{\sqrt{2}}$$

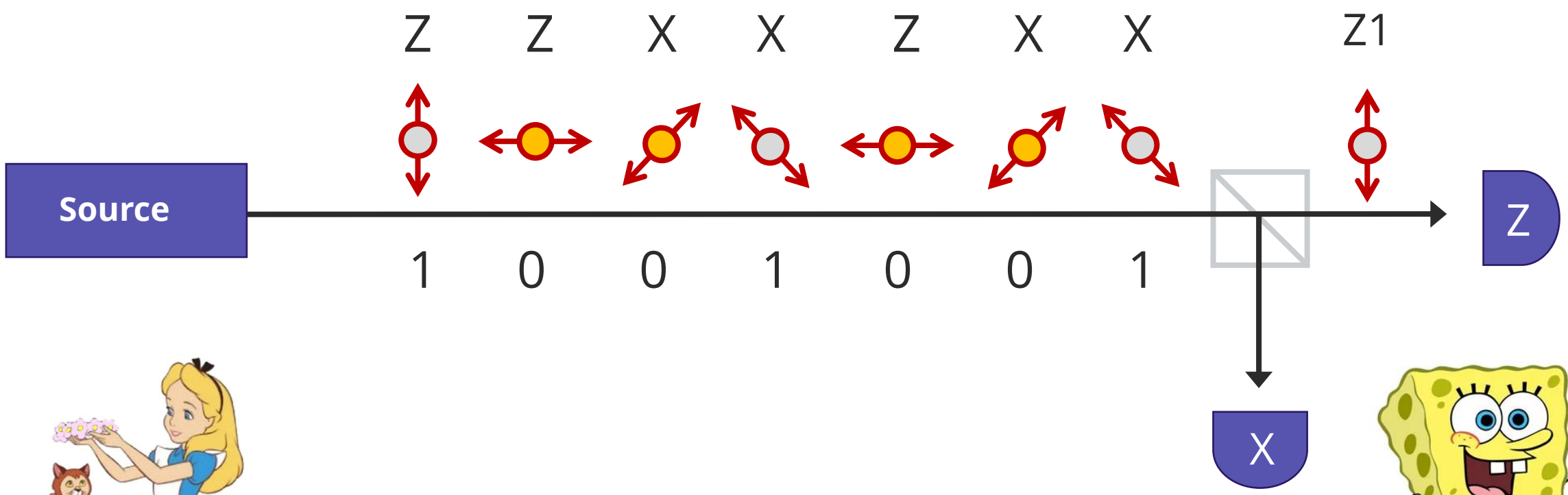


- Maximum uncertainty

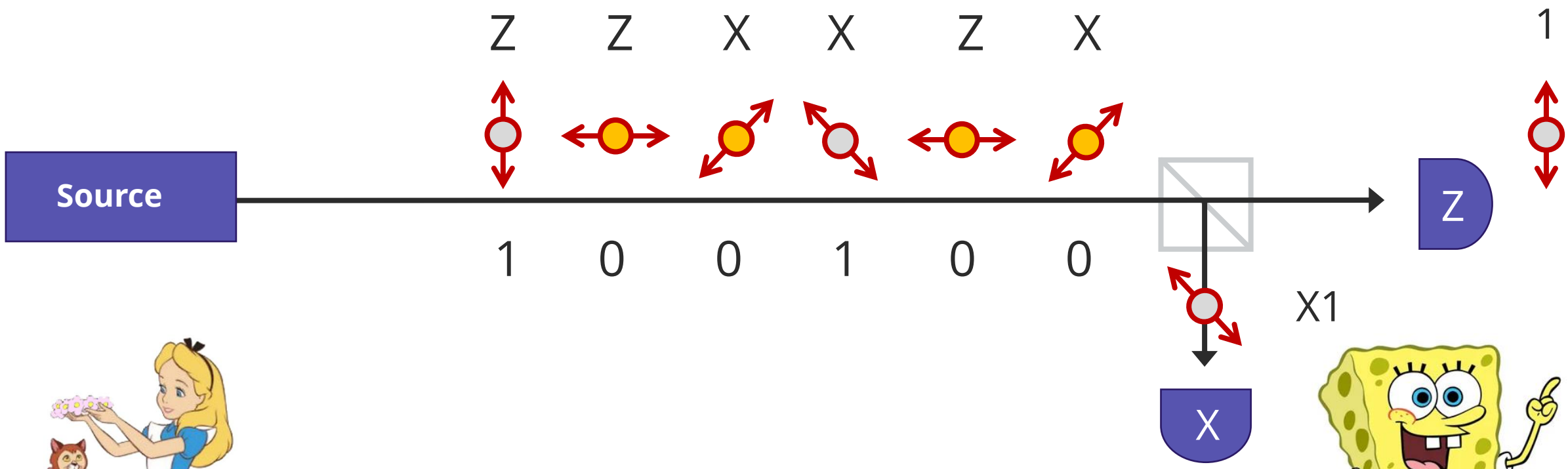
Prepare and Measure



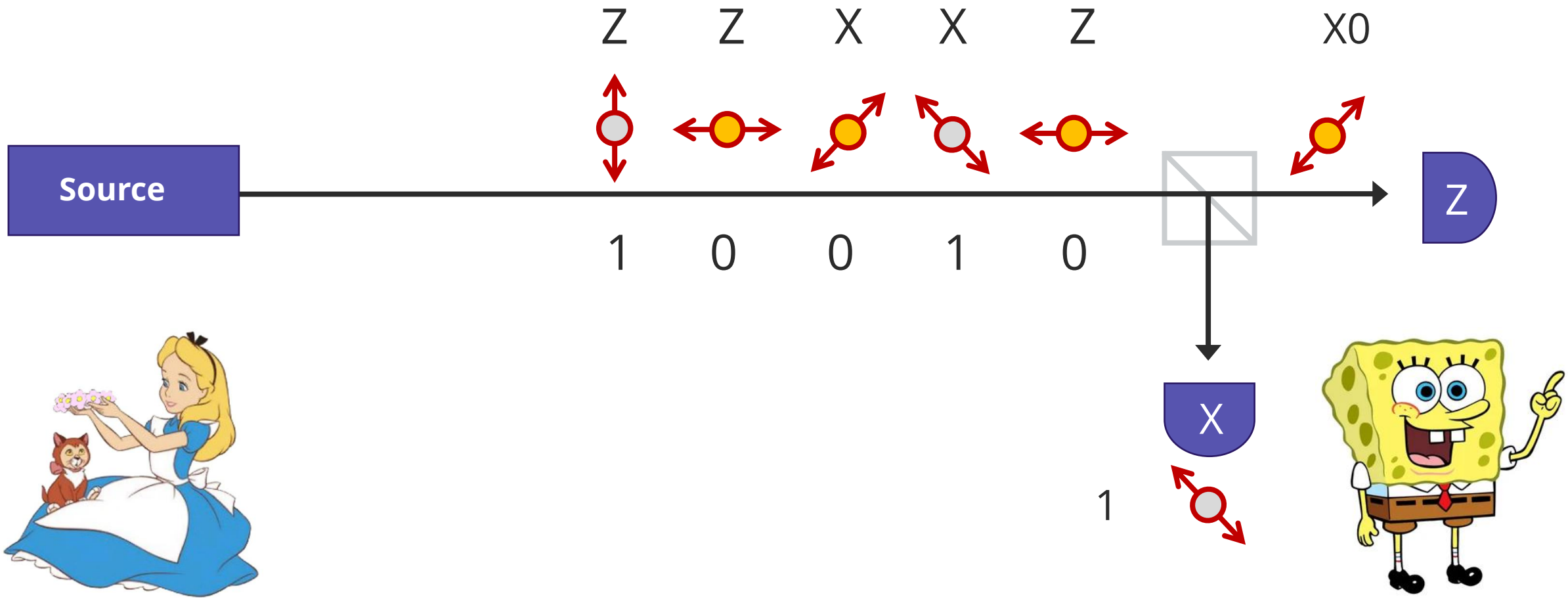
Prepare and Measure



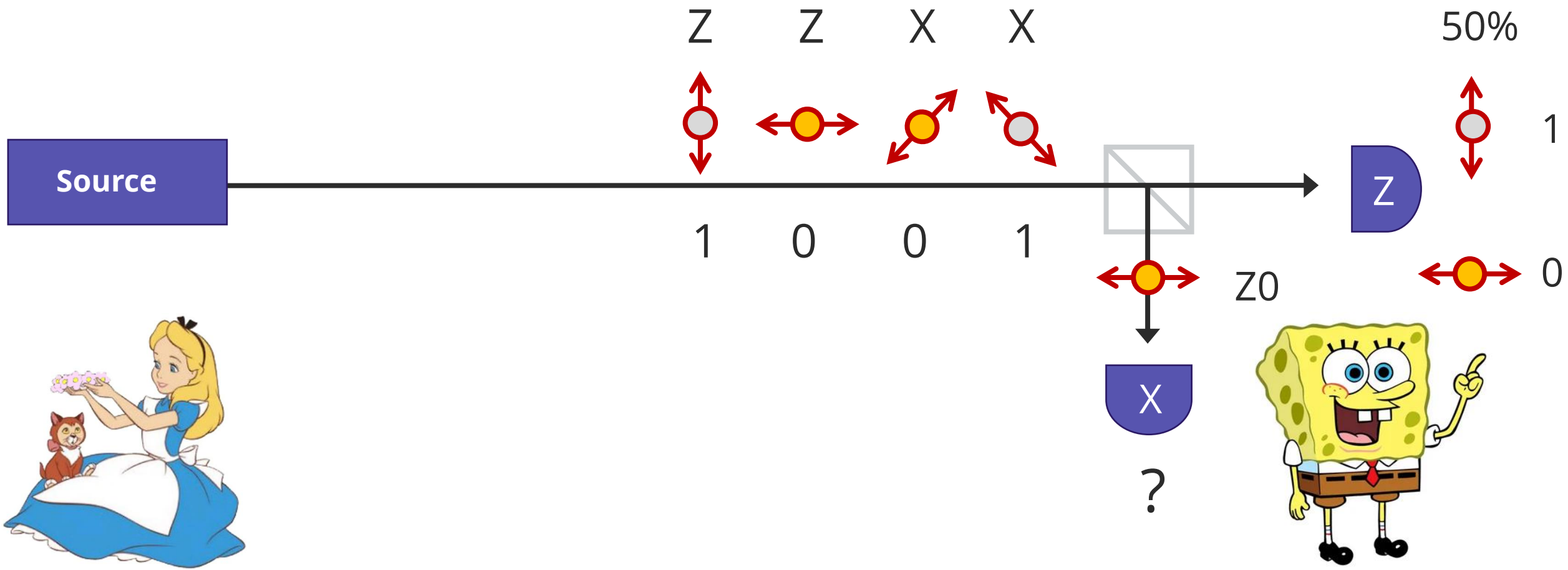
Prepare and Measure



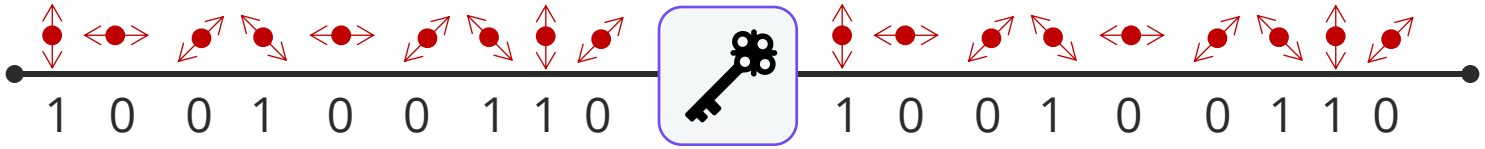
Prepare and Measure

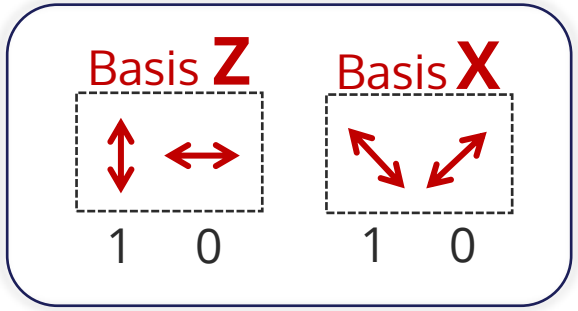


Prepare and Measure

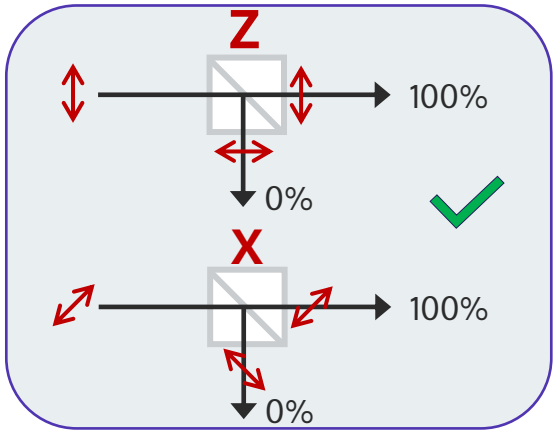


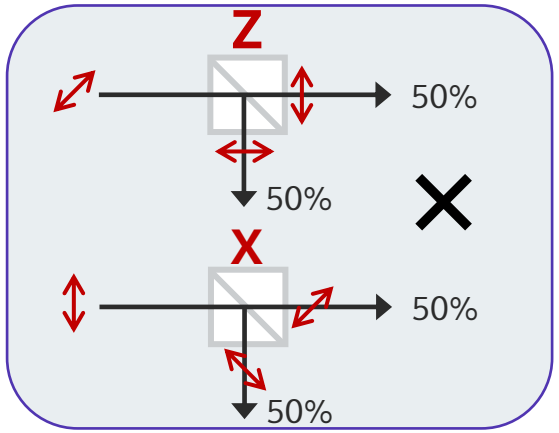
Quantum communication



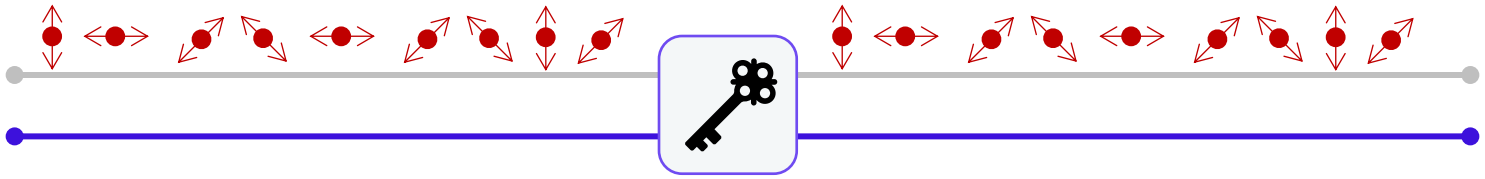


Quantum Measurements





Classical Channel



Alice

Bob

Quantum communication

Prep. and meas. of quantum states,
distributed in the quantum channel

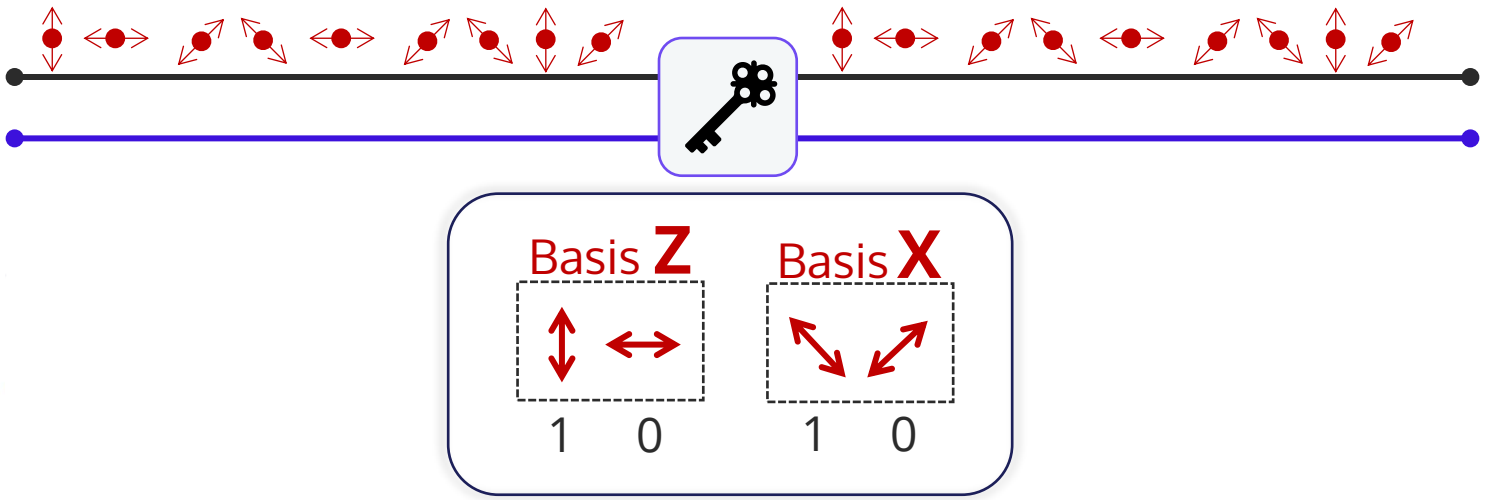
Classical post-processing

Elaboration of quantum results
via public discussion in the classical channel
(short-term authentication)

Secure key
k

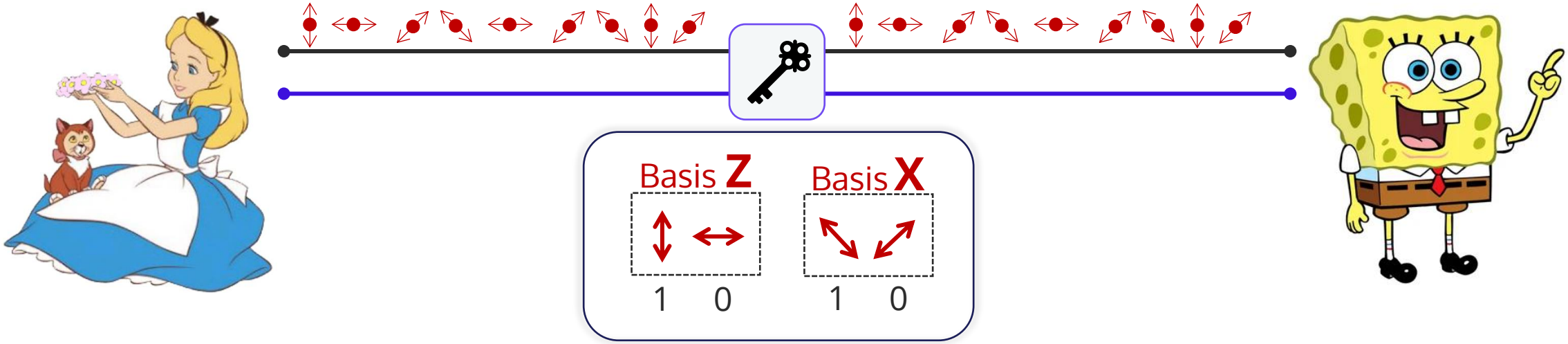
Secure key
k

Sifting (bases riconciliation)



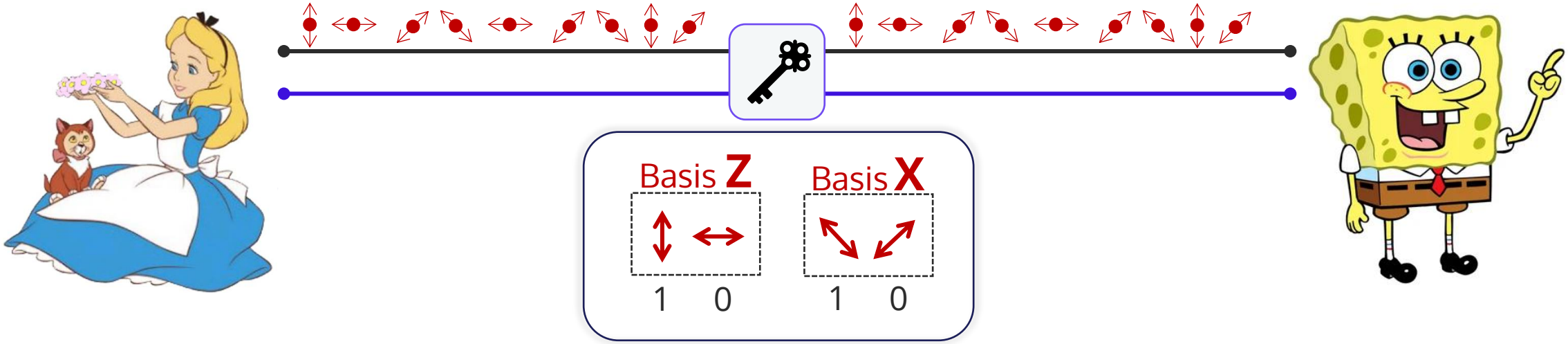
Alice	basis	Z	Z	X	X	Z	X	X	Z
	state	↕	↔	↗	↘	↔	↗	↘	↕
	bit	1	0	0	1	0	0	1	1
Bob	basis	Z	X	Z	X	X	X	Z	Z
	state	↕	↗	↕	↘	↘	↗	↕	↕
	bit	1	0	1	1	1	0	1	1

Sifting (bases riconciliation)



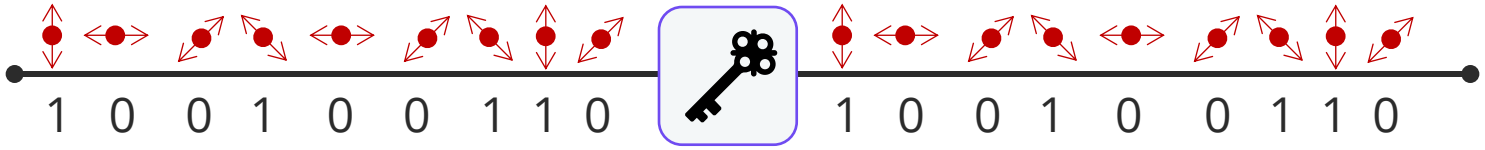
Alice	basis	Z	Z	X	X	Z	X	X	Z
	state	↕	↔	⤢	⤡	↔	⤢	⤡	↕
	bit	1	0	0	1	0	0	1	1
Bob	basis	Z	X	Z	X	X	X	Z	Z
	state	↕	⤢	↕	⤡	⤡	⤢	↕	↕
	bit	1	0	1	1	1	0	1	1
			✗✓	✗✗		✗✗		✗✓	

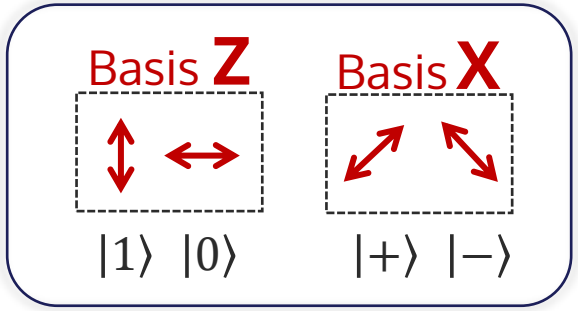
Sifting (bases riconciliation)



Alice	basis	**Z**	Z	X	**X**	Z	**X**	X	**Z**	public
	state	↕	↔	↗	↘	↔	↗	↘	↕	
	bit	1	0	0	1	0	0	1	1	
Bob	basis	**Z**	X	Z	**X**	X	**X**	Z	**Z**	public
	state	↕	↗	↕	↘	↘	↗	↕	↕	
	bit	1	0	1	1	1	0	1	1	
Sifted key		**1**	**--**	**--**	**1**	**--**	**0**	**--**	**1**	

Quantum communication





Quantum Superposition

$$\nearrow\!\!\searrow = \frac{\leftrightarrow + \updownarrow}{\sqrt{2}}$$

$$\nwarrow\!\!\searrow = \frac{\leftrightarrow - \updownarrow}{\sqrt{2}}$$

Bra-ket notation

$$|+\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}}$$

$$|-\rangle = \frac{|0\rangle - |1\rangle}{\sqrt{2}}$$

Max unbiased basis

$$\Pr(out_j) = |\langle j|i\rangle|^2 = \frac{1}{2}$$

$$j \in \{+,-\}, i \in \{0,1\}$$

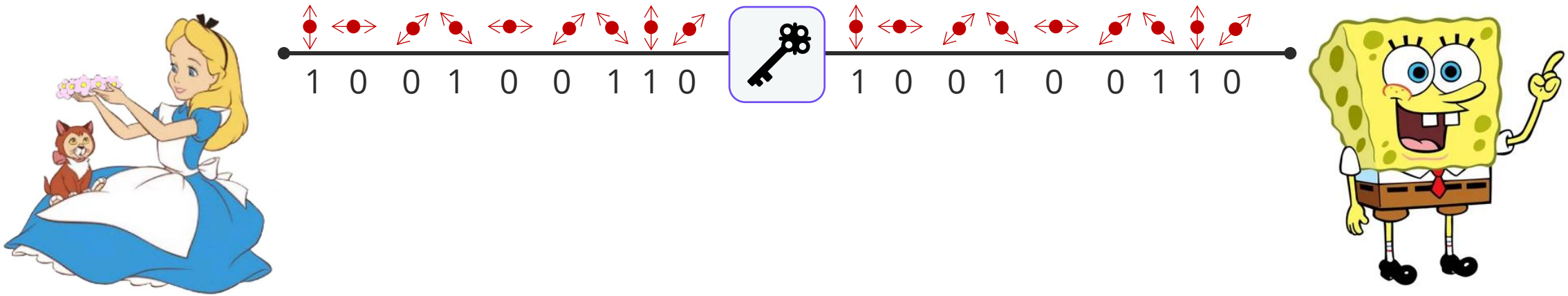
Tensor Spaces

State: $|1\rangle_A \in H_A$

Superposition: $|+\rangle_A = \frac{|0\rangle_A + |1\rangle_A}{\sqrt{2}} \in H_A$

(Separable) composite state: $|k_2\rangle_A = \updownarrow \otimes \updownarrow = |1\rangle_A \otimes |1\rangle_A = |11\rangle_A \in H_A \otimes H_A$

Quantum communication



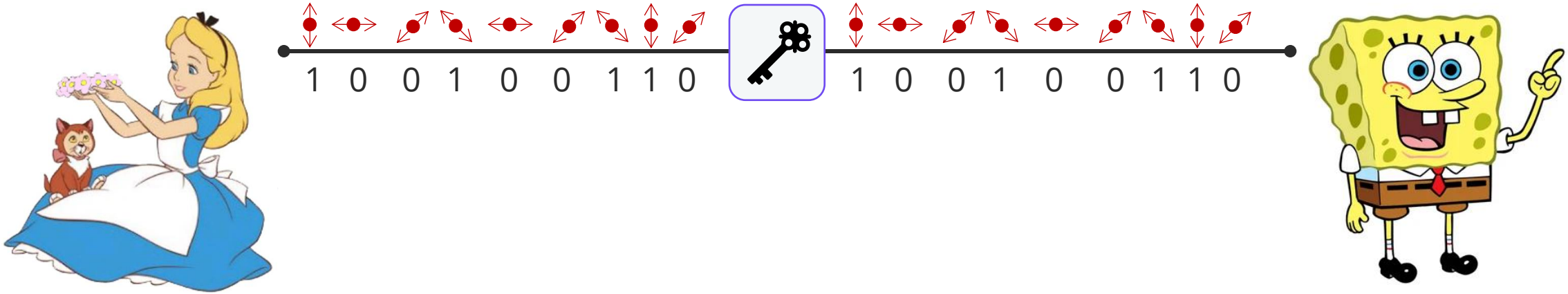
Alice state: $|1\rangle_A \otimes |0\rangle_A \otimes |+\rangle_A \otimes |-\rangle_A \otimes |0\rangle_A \otimes |+\rangle_A \otimes |-\rangle_A \otimes |1\rangle_A$

Classical bits: $k_A = (1,0,0,1,0,0,1,1)$

Bob state: $|1\rangle_B \otimes |+\rangle_B \otimes |1\rangle_B \otimes |-\rangle_B \otimes |-\rangle_B \otimes |+\rangle_B \otimes |1\rangle_B \otimes |1\rangle_B$

Classical bits: $k_B = (1,0,1,1,1,0,1,1)$

Quantum communication



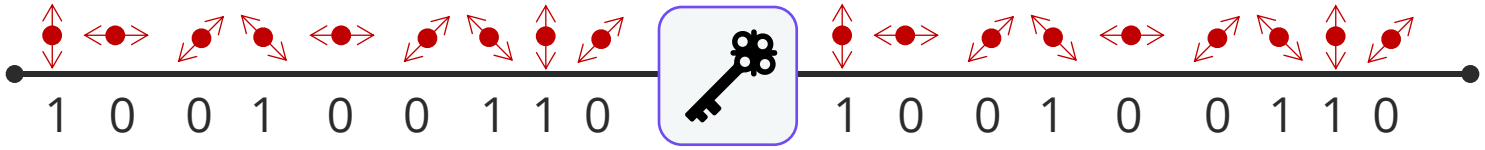
Alice state: $|1\rangle_A \otimes |0\rangle_A \otimes |+\rangle_A \otimes |-\rangle_A \otimes |0\rangle_A \otimes |+\rangle_A \otimes |-\rangle_A \otimes |1\rangle_A$

Classical bits: $k_A = (1,0,0,1,0,0,1,1)$

Bob state: $|1\rangle_B \otimes |+\rangle_B \otimes |1\rangle_B \otimes |-\rangle_B \otimes |-\rangle_B \otimes |+\rangle_B \otimes |1\rangle_B \otimes |1\rangle_B$

Classical bits: $k_B = (1,0,1,1,1,0,1,1)$

Quantum communication + Sifting



Alice state: $|1\rangle_A \otimes |0\rangle_A \otimes |+\rangle_A \otimes |-\rangle_A \otimes |0\rangle_A \otimes |+\rangle_A \otimes |-\rangle_A \otimes |1\rangle_A$

Classical bits: $k_A = (1,0,1,1)$

Bob state: $|1\rangle_B \otimes |+\rangle_B \otimes |1\rangle_B \otimes |-\rangle_B \otimes |-\rangle_B \otimes |+\rangle_B \otimes |1\rangle_B \otimes |1\rangle_B$

Classical bits: $k_B = (1,1,0,1)$

After sifting $k_A = k_B = (1,1,0,1)$

Density matrix notation

Let $|\phi\rangle \in H$.

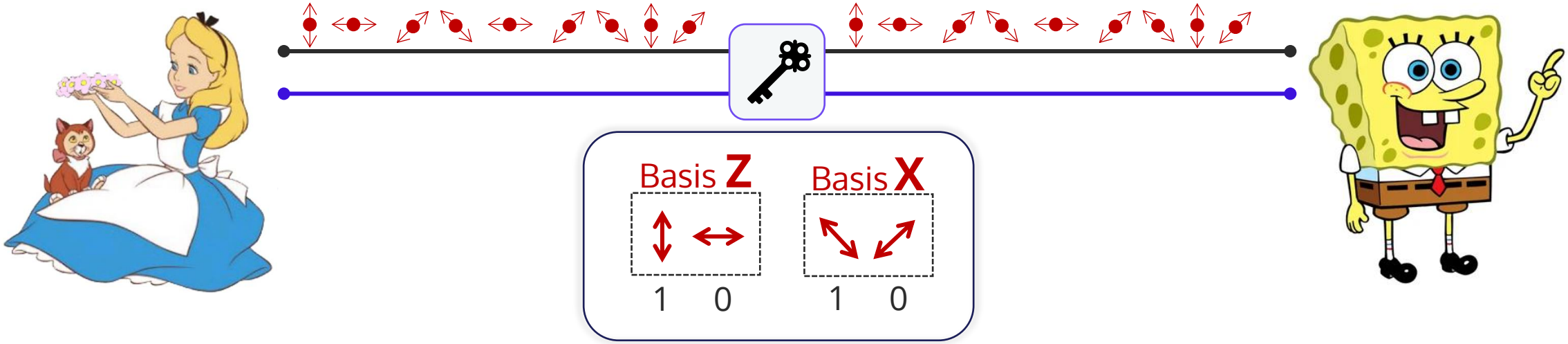
Bra notation: $\langle\phi| = |\phi\rangle^{\dagger}$, (transpose-conjugate).
Then $|\phi\rangle \otimes \langle\phi| =: |\phi\rangle\langle\phi| \in H \otimes H^{*}$ is an operator, called density matrix.

- A state is pure if its density matrix has the form $\rho = |\phi\rangle\langle\phi|$
- Otherwise, it is a (classical) statistical mixture

$$\rho = \sum_i \alpha_i |\phi_i\rangle\langle\phi_i|, \quad \text{with } \sum_i \alpha_i = 1.$$

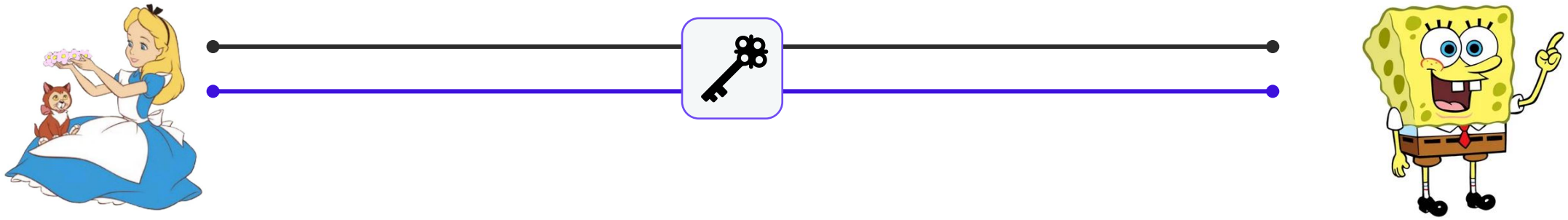
The density matrix formalism gives a (general) description of the state.

Sifting (bases riconciliation)



Alice	basis	**Z**	Z	X	**X**	Z	**X**	X	**Z**	public
	state	↕	↔	↗	↘	↔	↗	↘	↕	
	bit	1	0	0	1	0	0	1	1	
Bob	basis	**Z**	X	Z	**X**	X	**X**	Z	**Z**	public
	state	↕	↗	↕	↘	↘	↗	↕	↕	
	bit	1	0	1	1	1	0	1	1	
Sifted key		**1**	**--**	**--**	**1**	**--**	**0**	**--**	**1**	

They expect

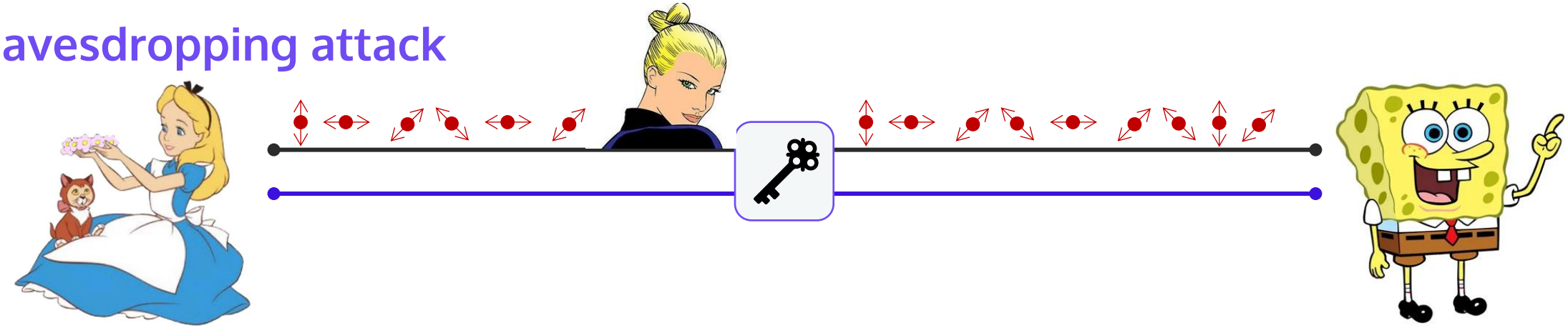


Let $K_A = K_B = K = \{0,1\}^N$ be the space of binary key of length N, $|K| = 2^N$.
Alice and Bob expect a (copy of a) shared key

$$\rho_{A,B}^{N,ideal} := \frac{1}{|K|} \sum_{k \in K} |k\rangle_{K_A}\langle k| \otimes |k\rangle_{K_B}\langle k|$$

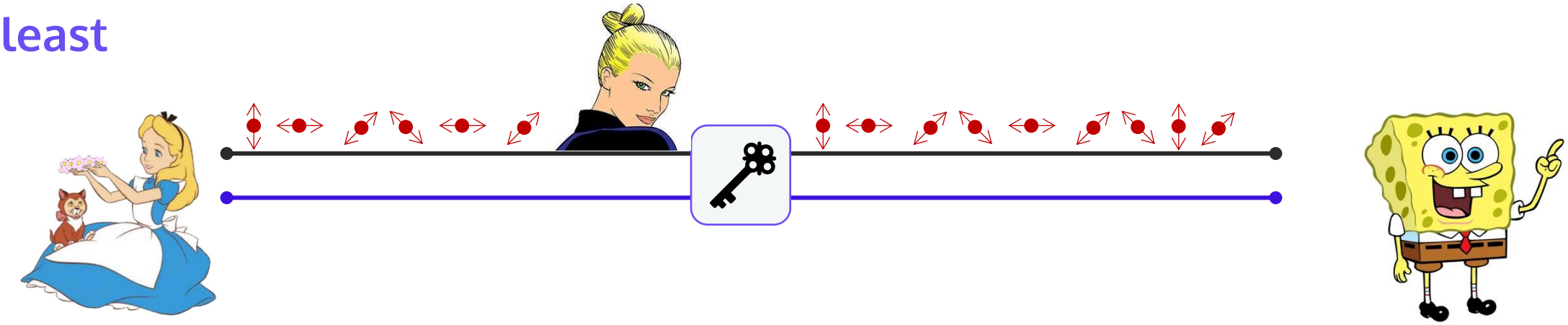
→ the maximally correlated keys.
(Remember e.g. $|k\rangle = |010001101010\rangle$ of length N)

Eavesdropping attack



Alice	basis	Z	Z	X	X	Z	X	X	Z
	state	↕	↔	↗	↘	↔	↗	↘	↕
	bit	1	0	0	1	0	0	1	1
Eve	basis	Z	Z	Z	Z	X	X	X	X
	state	↕	↔	↕	↔	↘	↗	↘	↗
	bit	1	0	1	0	1	0	1	0
Bob	basis	Z	X	Z	X	X	X	Z	Z
	state	↕	↗	↕	↗	↘	↗	↕	↕
	bit	1	0	1	0	1	0	1	1
Sifted key		**1**	**--**	**--**	**Error**	**--**	**0**	**--**	**1**

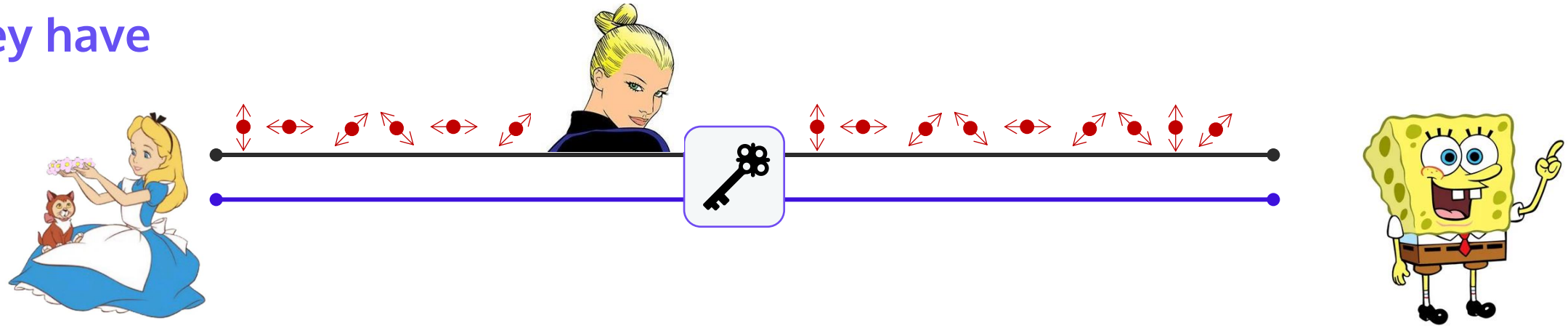
At least



At least

$$\rho_{A,B}^{N,ideal} := \frac{1}{|K|}\sum_{k\in K}(|k\rangle_A\langle k| \otimes |k\rangle_B\langle k|) \otimes \rho_E$$

They have



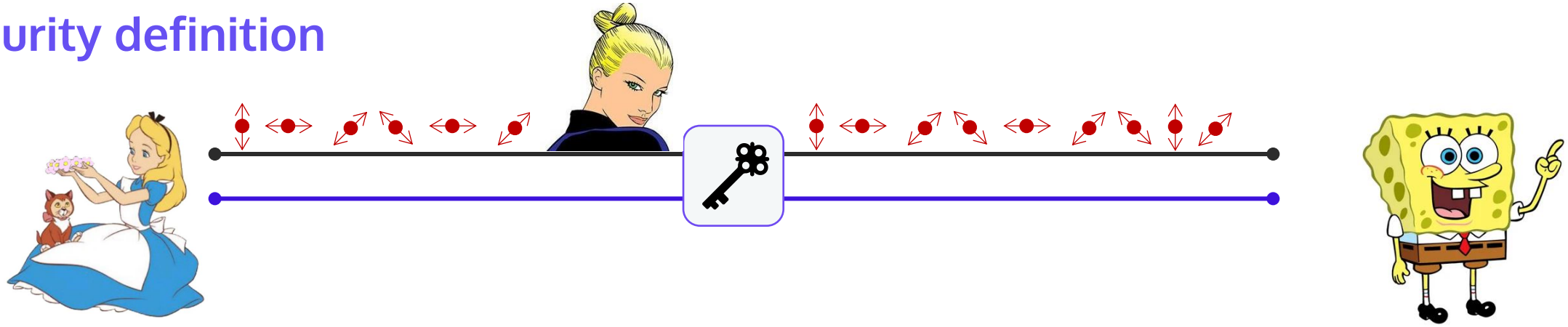
Let $K_A = K_B = K = \{0,1\}^N$ be the space of binary key of length N, $|K| = 2^N$.
Alice and Bob (and Eve) have the state of the form:

$$\rho^N_{A,B,E} = \sum_{k_A,k_B \in K} P_{k_A,k_B} |k_A\rangle_{K_A}\langle k_A| \otimes |k_B\rangle_{K_B}\langle k_B| \otimes \rho_E^{(k_A,k_B)}$$

with $\rho_E^{(k_A,k_B)} \in H_E$, Eve's final conditioned side-information.

In general: $\neq \rho^{N,ideal}_{A,B} = \frac{1}{|K|}\sum_{k\in K}(|k\rangle_A\langle k| \otimes |k\rangle_B\langle k|) \otimes \rho_E$

Security definition



At the end of a QKD protocol, Alice and Bob hold the final keys, while Eve has a final side-information. Let $\epsilon_{sec} \in [0,1]$.
We say the protocol is ϵ_{sec}-secure if

$$d\left(\rho_{A,B,E}^{\ell}, \rho_{A,B}^{\ell,ideal} \otimes \rho_E\right) \leq \epsilon_{sec}$$

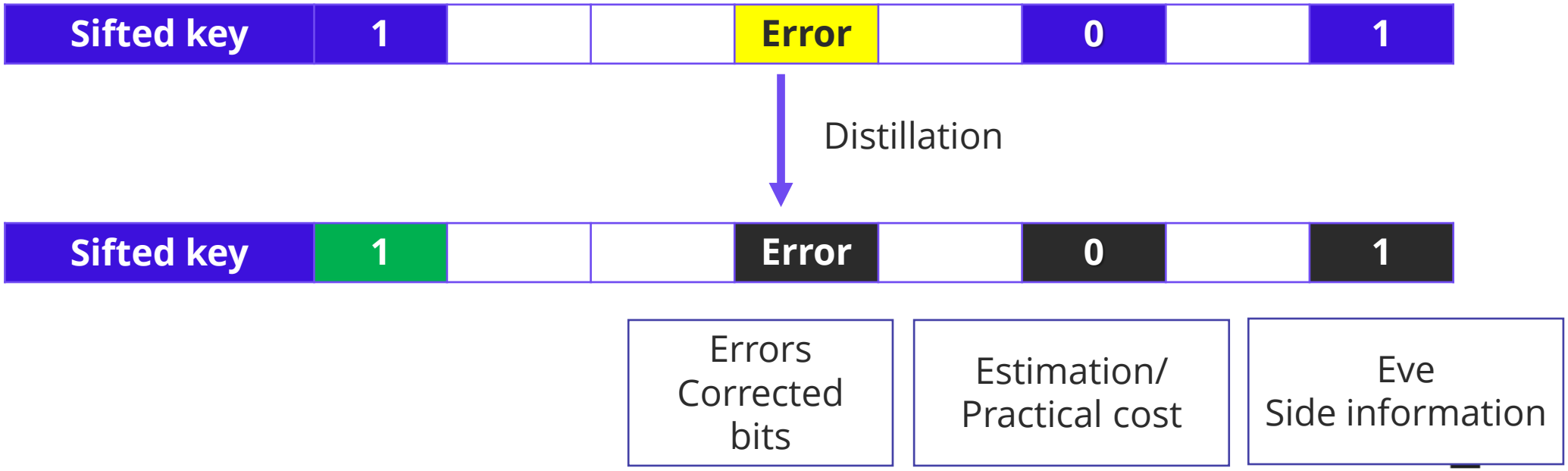
→ Quantification of distinguishability

Main considerations

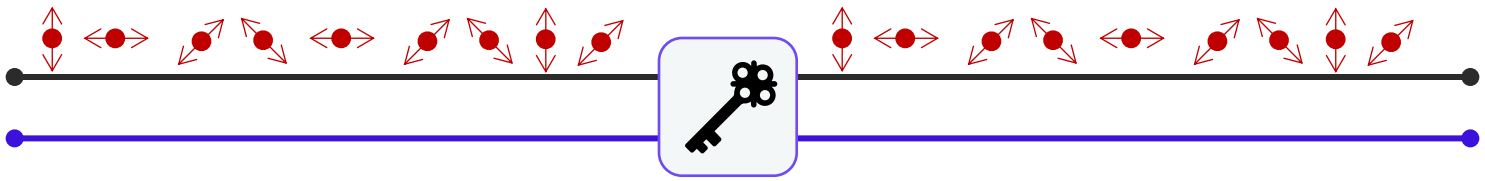
The ***tensor*** $\rho_{A,B,E}$ is the real (not ideal) state:

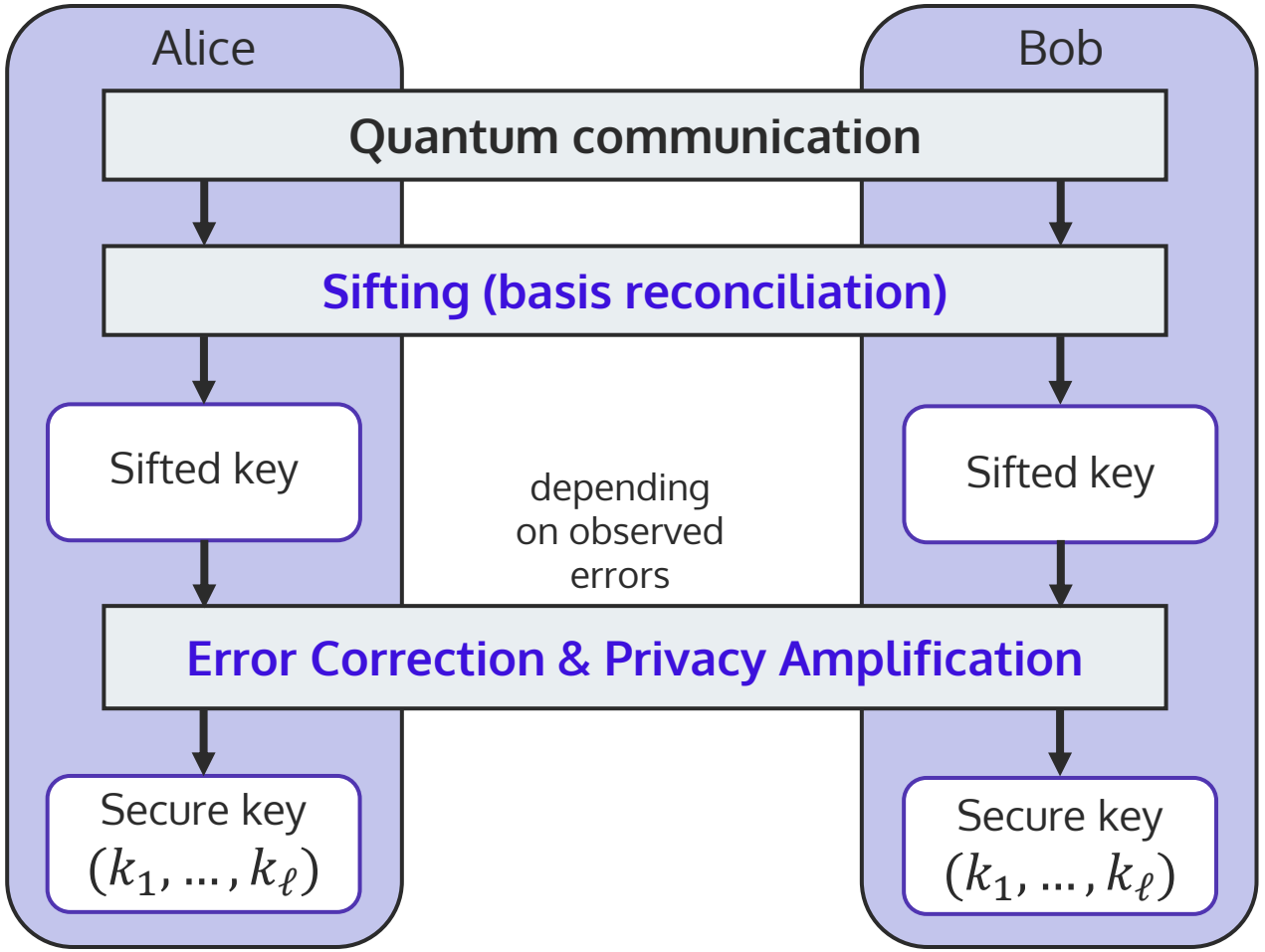
- It includes modelled attacks (if specifically assumed) + *setup imperfections*

- From the model, you must
  - *Find* errors → correct them
  - *Estimate* (bounds on) Eve's information → privacy amplify to ℓ

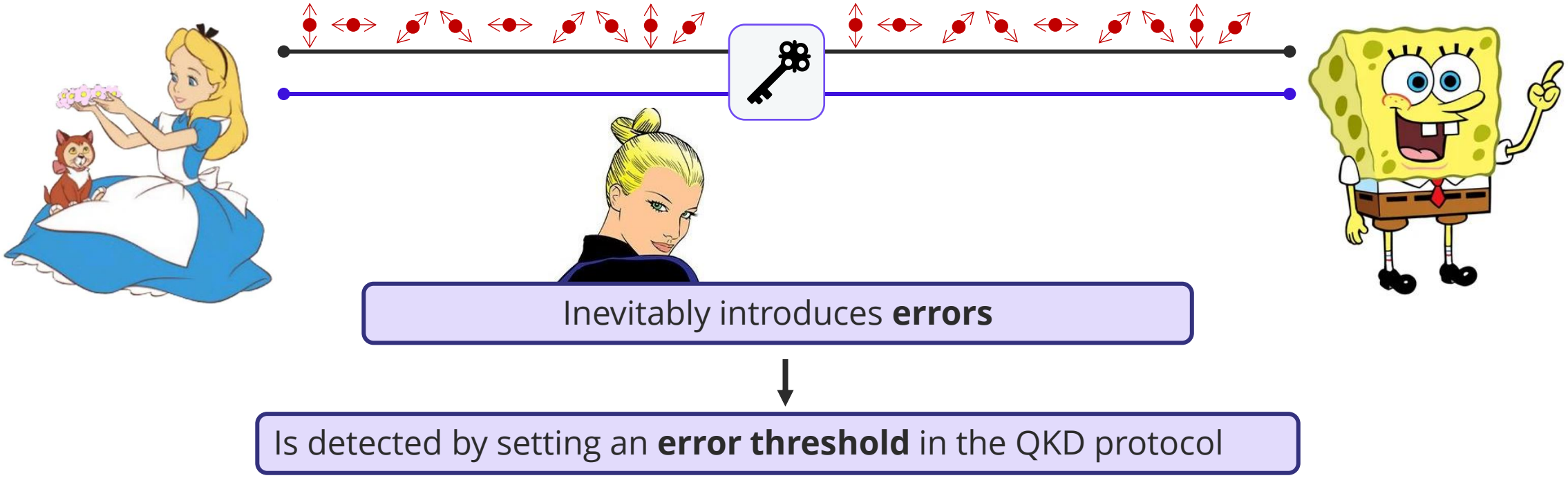


Quantum Key Distribution protocol





Eavesdropping attack and security



- Errors < threshold → **security is improved** reducing the final key length
- Errors > threshold → protocol is **aborted**
- In both cases, **no useful information** is acquired by Eve in the end.

References

- Bennett and Brassard, *Quantum cryptography: Public key distribution and coin tossing*, Theoretical computer science (2014)
- Fung and Lo, *Security proof of a three-state quantum-key-distribution protocol without rotational symmetry,* Phys. Rev. A (2006)
- Tupkary, Tan, Nahar, Kamin, Lütkenhaus, *QKD security proofs for decoy-state BB84: protocol variations, proof techniques, gaps and limitations,* arXiv:2502.10340 (2025)
- Vagniluca*, High-dimensional protocols for practical quantum key distribution over metropolitan fiber links,* PhD Thesis, (2021)

Thank you