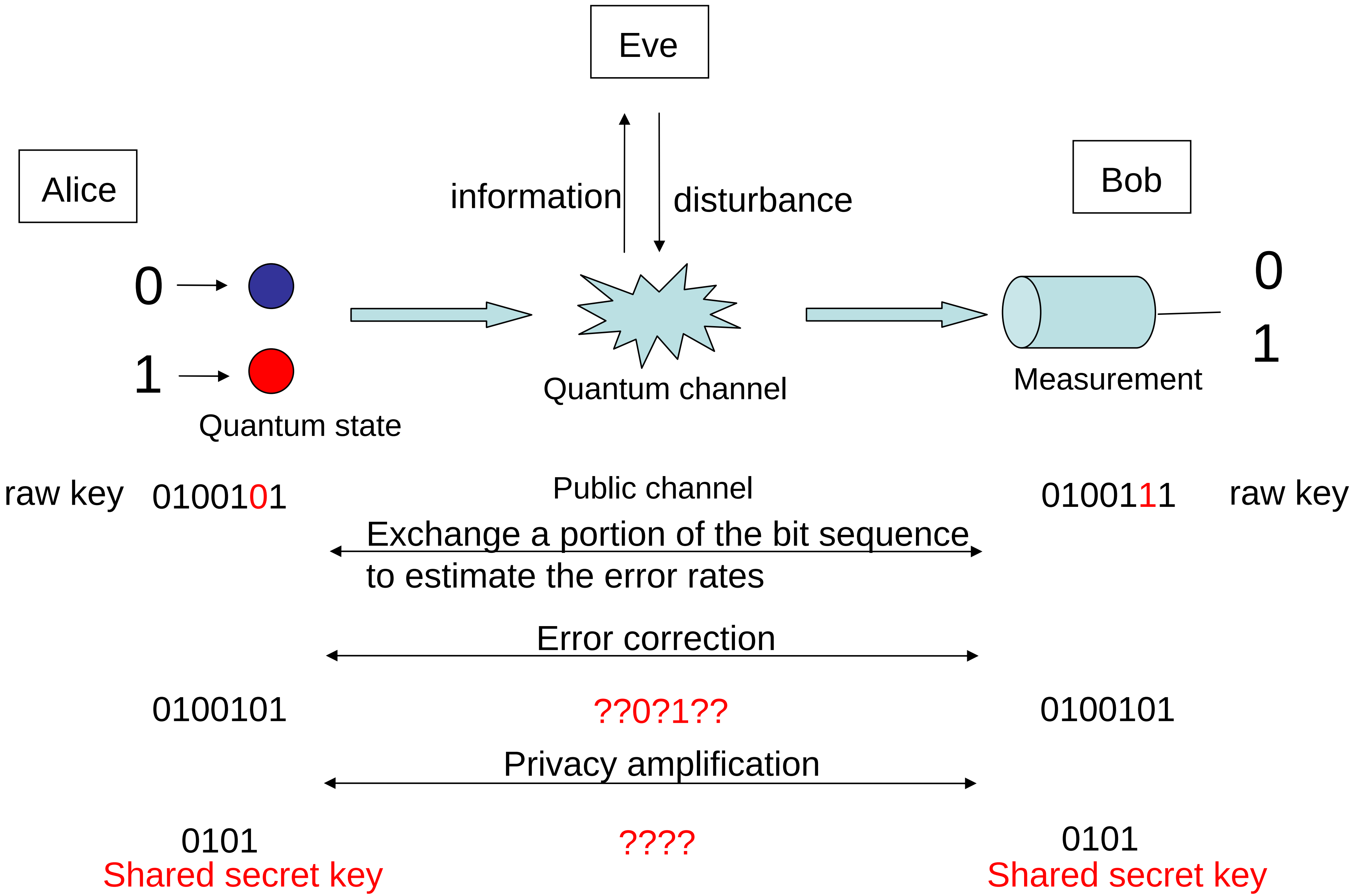
ICITS2009, Shizuoka, Japan (Dec. 4)

Security of key distribution and complementarity in quantum mechanics

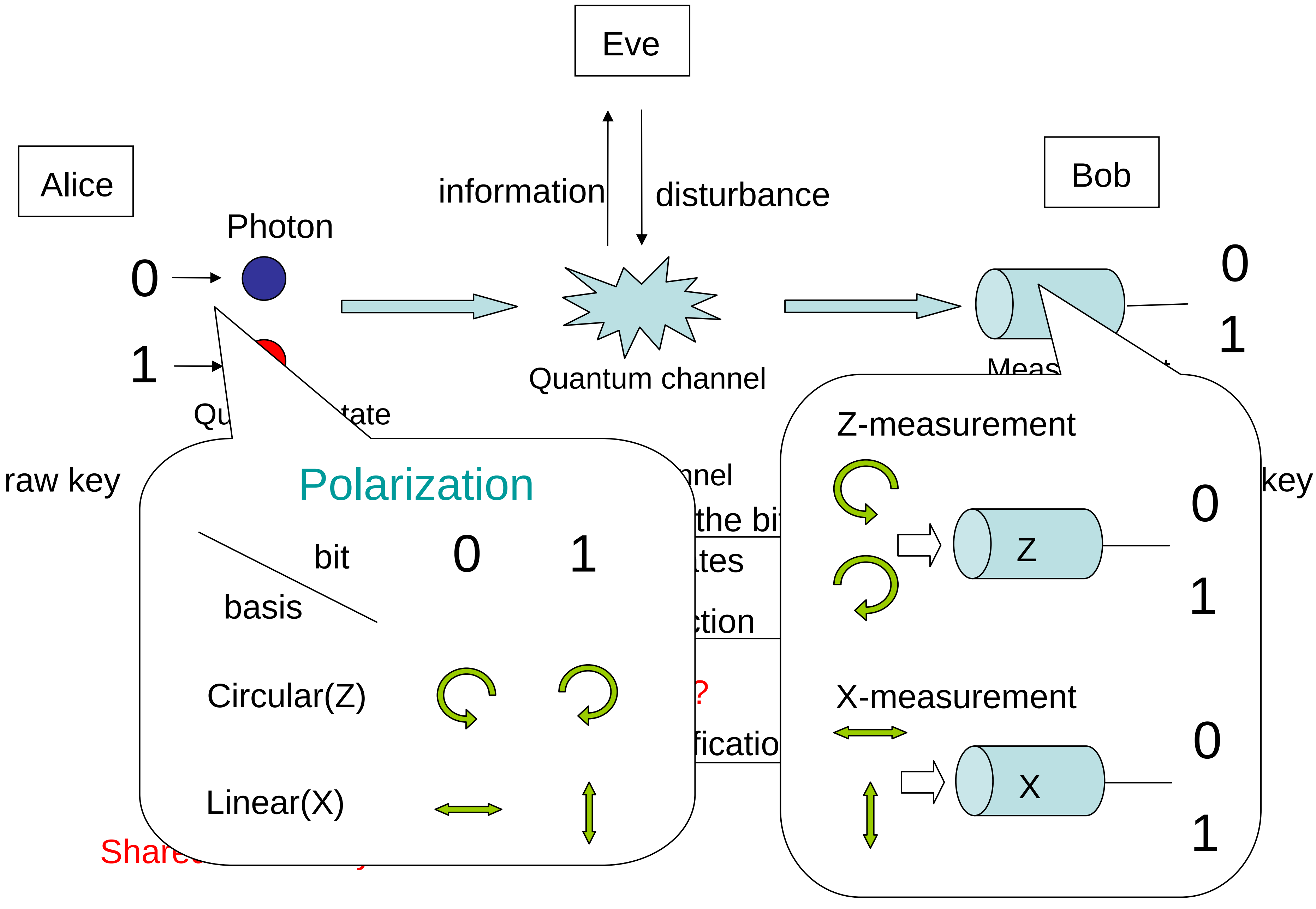
Osaka Univ. Masato Koashi

- Quantum key distribution (BB84 protocol)
- The goal of security proof
- A very short course of quantum mechanics
- Proving the security of QKD via complementarity
  - Basic idea
  - Small imperfections
  - A prescription for proving the security
- The security of the BB84 protocol
- Merits in the complementarity approach

Quantum key distribution (QKD)



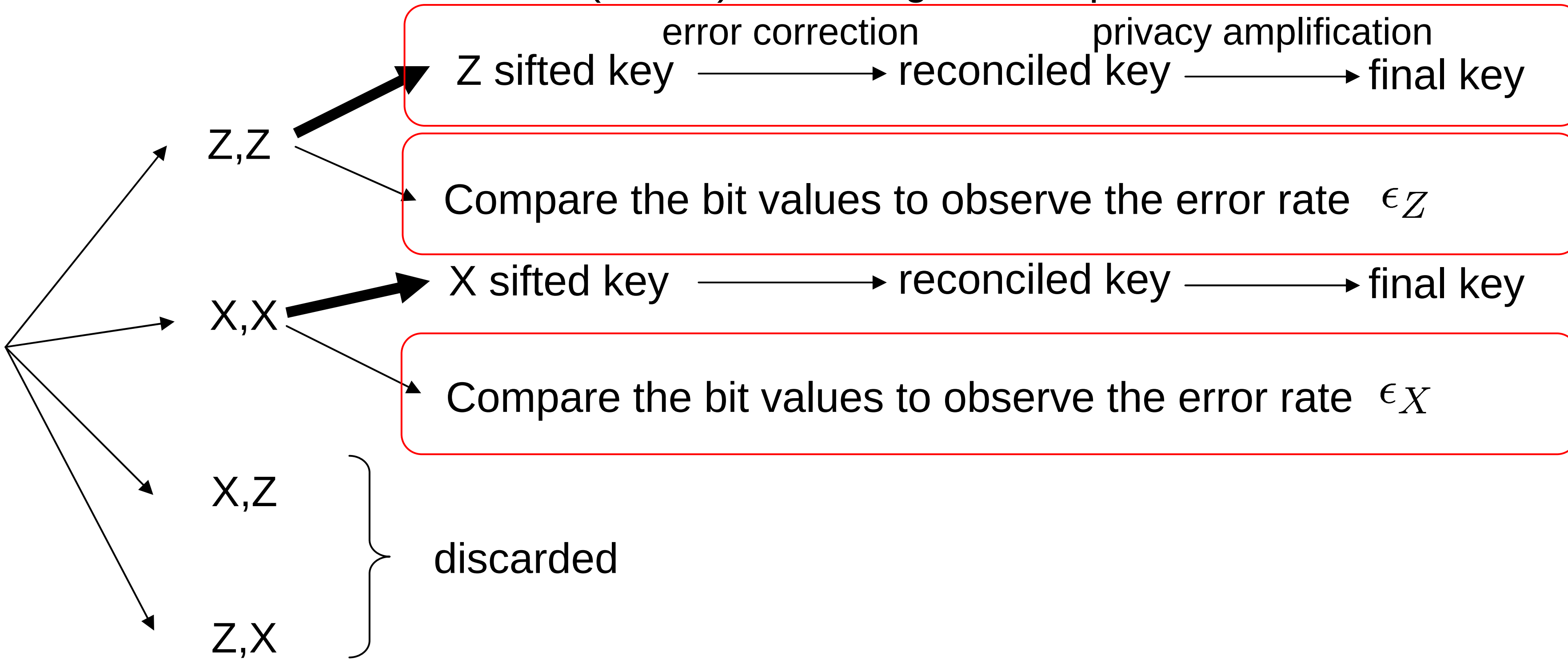
Bennett-Brassard 1984 (BB84) protocol



BB84 protocol

Alice chooses her basis (Z or X) according to fixed probabilities (e.g., 50% each).

Bob chooses his measurement (Z or X) according to fixed probabilities.

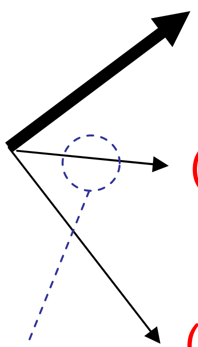


After Bob has received the photon (=Eve's attack has ended), Alice and Bob reveals their basis choices in public discussions.

BB84 protocol

Net key gain: $N(1 - h_X - h_Z)$

Encrypted communication of Nh_Z bits
to correct Bob's sifted key to match with Alice's.



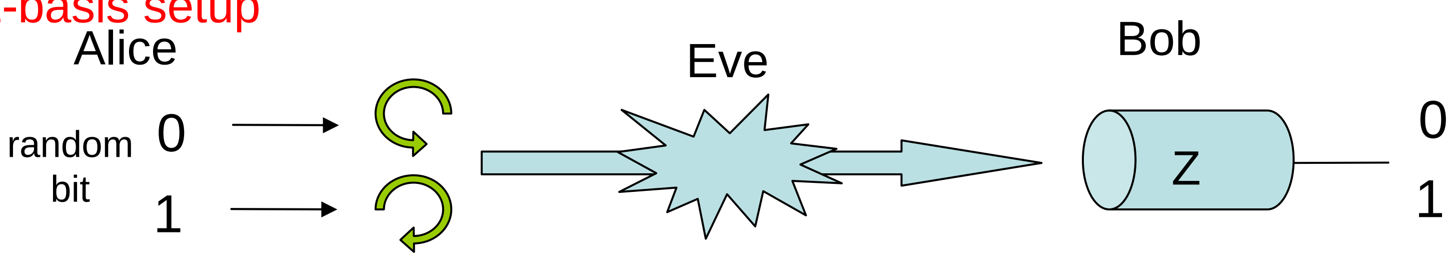
Z sifted key N bits $\xrightarrow{\text{error correction}}$ reconciled key N bits $\xrightarrow{\text{privacy amplification}}$ final key $N(1-h_X)$ bits

Compare the bit values to observe the error rate ϵ_Z

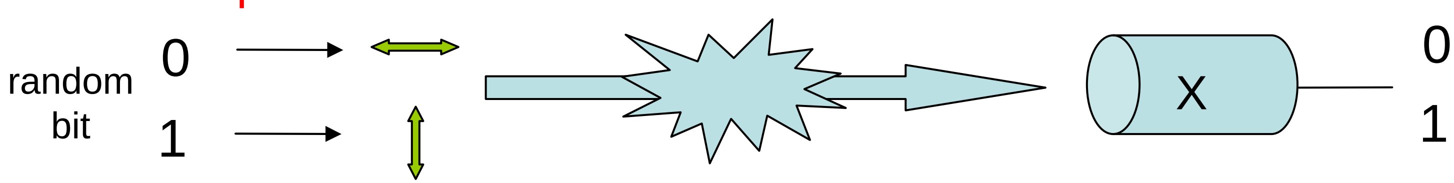
Compare the bit values to observe the error rate ϵ_X

Fair sampling
(No control from Eve)

Z-basis setup



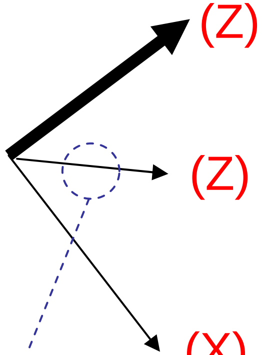
X-basis setup



BB84 protocol

Net key gain: $N(1-h_X-h_Z)$

Encrypted communication of Nh_Z bits
to correct Bob's sifted key to match with Alice's.



Z sifted key N bits $\xrightarrow{\text{error correction}}$ reconciled key N bits $\xrightarrow{\text{privacy amplification}}$ final key $N(1-h_X)$ bits

Compare the bit values to observe the error rate ϵ_Z

Compare the bit values to observe the error rate ϵ_X

Fair sampling
(No control from Eve)

Alice's reconciled key

Bob's reconciled key

Failure probability of error correction: $\delta_Z \equiv \Pr(\boldsymbol{Z} \neq \boldsymbol{Z}')$

$\delta_Z = \delta_Z(\epsilon_Z, h_Z)$ is determined by the error correction method and the theory of random sampling test.

Ideally, $\delta_Z \sim 0$ for $h_Z \sim H(\epsilon_Z)$

The goal of the security proof:

The imperfection in the final key : $\delta_{\text{key}}(\epsilon_Z, h_Z, \epsilon_X, h_X) \longleftarrow$ law of quantum mechanics

Quantum mechanics 101: States of a qubit

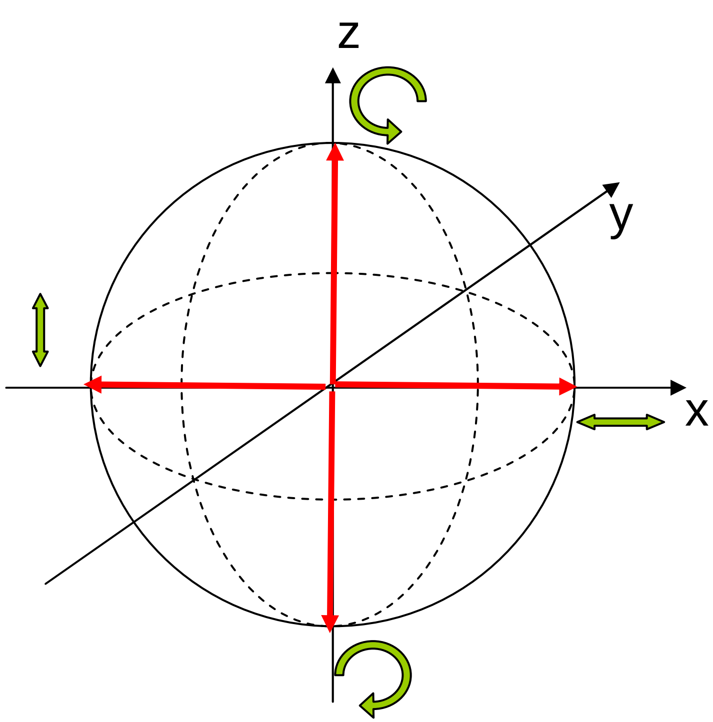
Qubit: the simplest of quantum systems

Any two-level system, such as polarization of a photon, and spin of an electron.

Pure states of a qubit $\longleftrightarrow$ 3D real vectors of unit length (Bloch vectors)

A ‘pure state’ should admit no finer description of the physical state.

(as opposed to a mixed state)



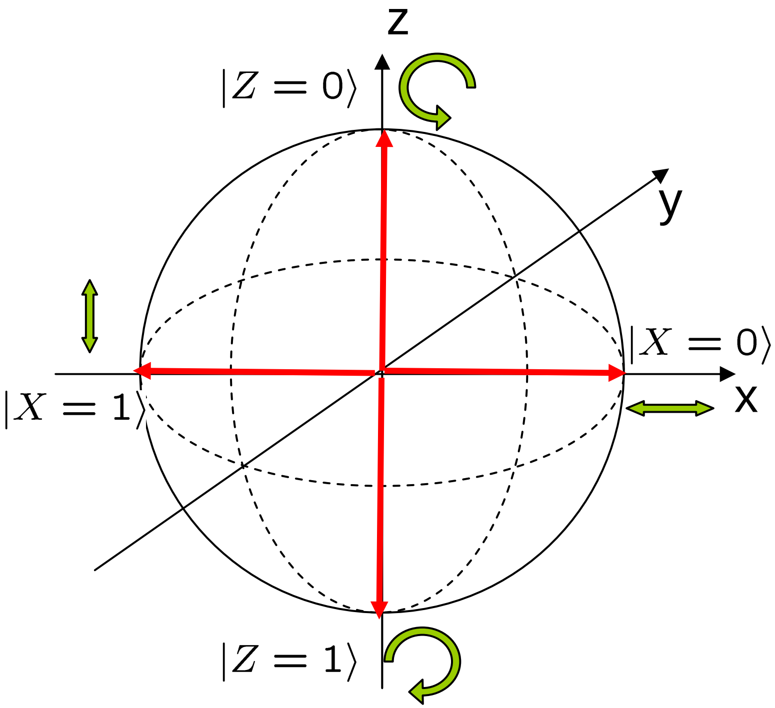
Spin ½ particle

Bloch vector = Spin vector

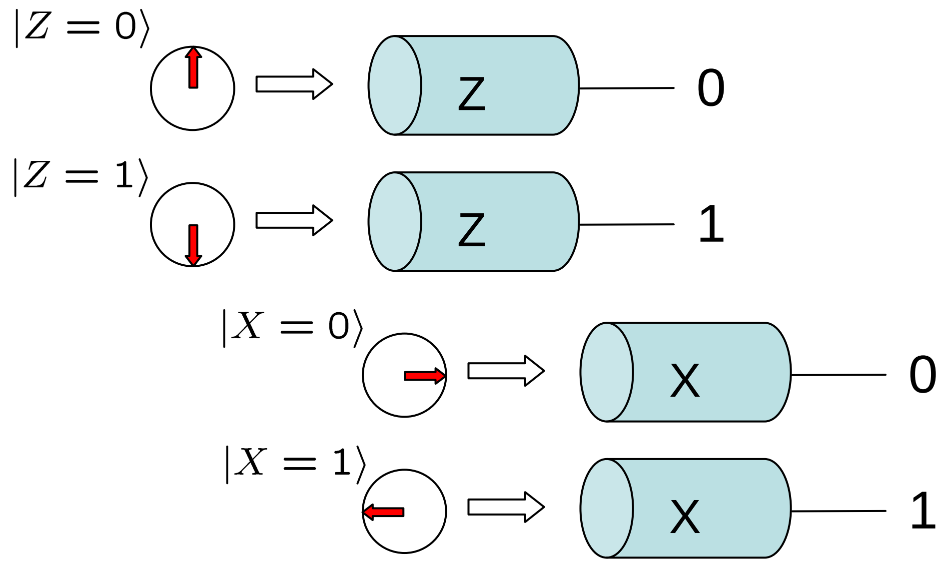
Photon polarization

Bloch sphere = Poincare sphere

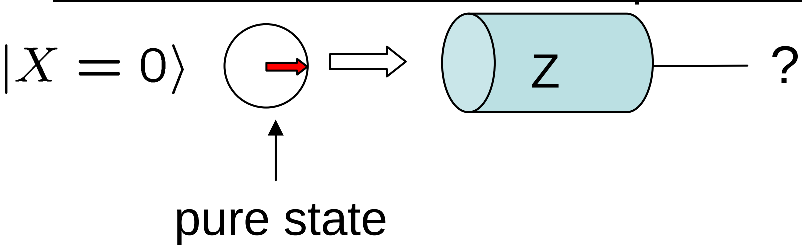
Quantum mechanics 101: Measurements



Two states with opposing Bloch vectors are perfectly distinguishable.



FACT: randomness from a pure state

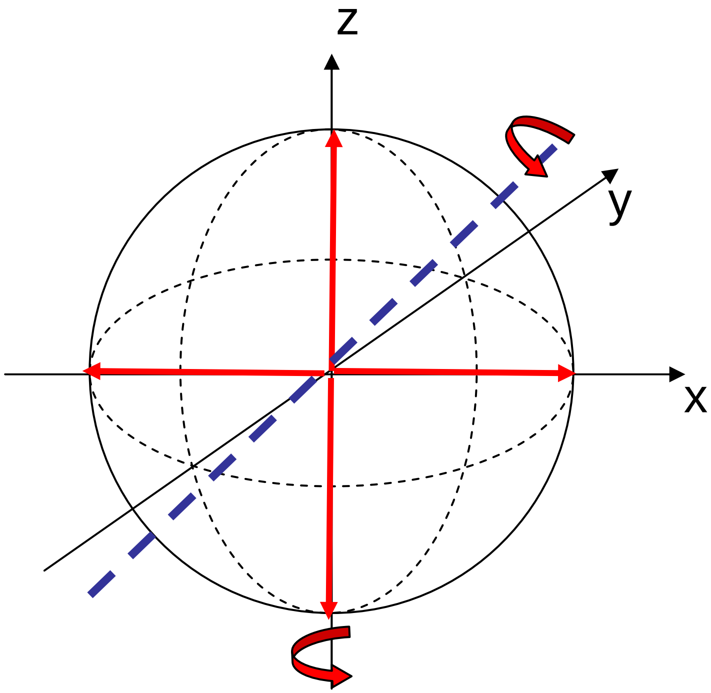


The outcome is a perfectly random bit.

No correlation to other systems

(A correlation would imply a finer description of the state.)

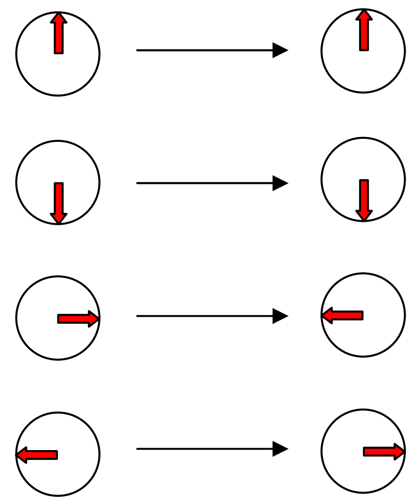
Quantum mechanics 101: Operation on a qubit



Any rotation of the Bloch sphere is a physically feasible transformation of states

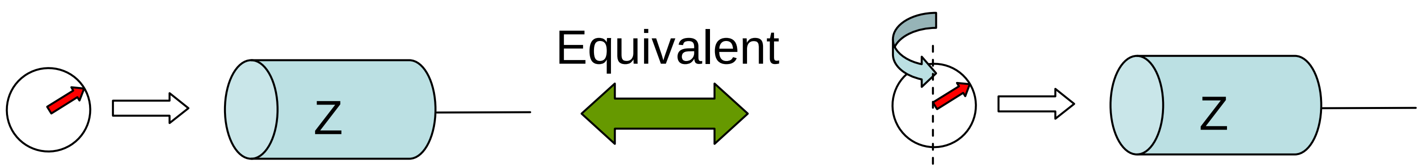
Electron spin: via magnetic field
Photon polarization: via wave plates

180 rotation around the z axis (Z rotation)



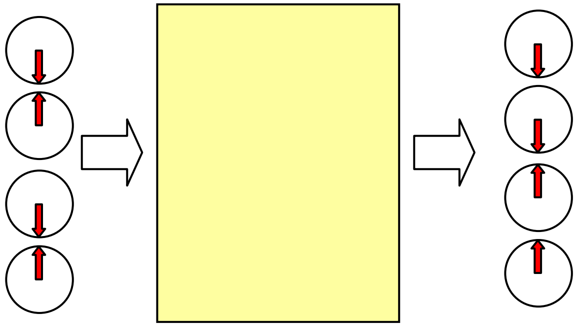
$\vert Z=0\rangle$	$\vert Z=0\rangle$
$\vert Z=1\rangle$	$\vert Z=1\rangle$
$\vert X=0\rangle$	$\vert X=1\rangle$
$\vert X=1\rangle$	$\vert X=0\rangle$

FACT: Z rotation does not affect Z measurement



Quantum mechanics 102: Interaction among qubits

$$|Z = 1010\rangle$$

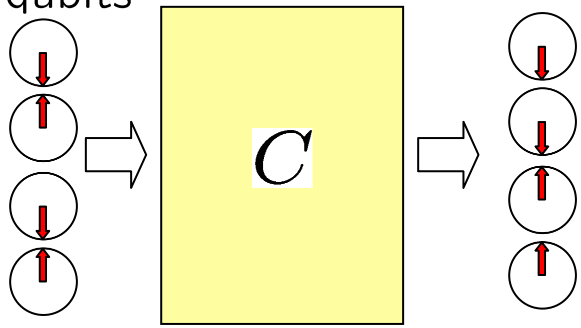


$$|Z = 1100\rangle$$

Quantum mechanics 102: Interaction among qubits

N qubits

$|\boldsymbol{Z} = \boldsymbol{z}\rangle$



$|\boldsymbol{Z} = \boldsymbol{z}C\rangle$

$C : (N \times N)$ invertible binary matrix

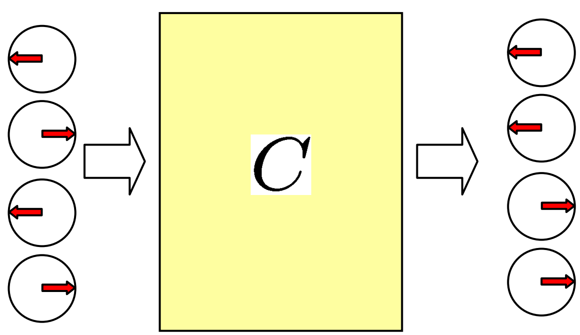
Reversible linear transformation of Z value

FACT:

For any C, there exists such a physical operation that is reversible, and also satisfies

...

$|\boldsymbol{X} = \boldsymbol{x}\rangle$



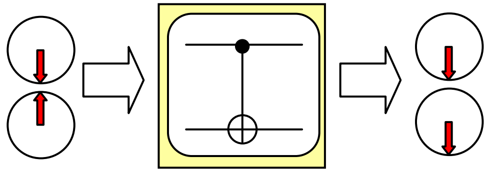
$|\boldsymbol{X} = \boldsymbol{x}(C^{-1})^T\rangle$

$$|\boldsymbol{X} = \boldsymbol{x}\rangle = N^{-1/2} \sum_{\boldsymbol{z}} (-1)^{\boldsymbol{x}\cdot\boldsymbol{z}} |\boldsymbol{Z} = \boldsymbol{z}\rangle$$

Quantum mechanics 102: Interaction among qubits

$C = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ (Controlled-NOT gate) $(C^{-1})^T = C^T = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$

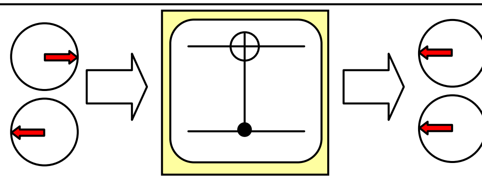
$|Z_1 = z_1\rangle$
$|Z_2 = z_2\rangle$



$|Z_1 = z_1\rangle$
$|Z_2 = z_1 + z_2\rangle$

$$|\boldsymbol{Z} = [z_1 z_2]\rangle \longrightarrow |\boldsymbol{Z} = [z_1 z_2]C\rangle$$

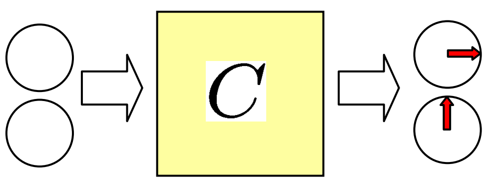
$|X_1 = x_1\rangle$
$|X_2 = x_2\rangle$



$|X_1 = x_1 + x_2\rangle$
$|X_2 = x_2\rangle$

$$|\boldsymbol{X} = [x_1 x_2]\rangle \longrightarrow |\boldsymbol{X} = [x_1 x_2](C^{-1})^T\rangle$$

$|?????\rangle$



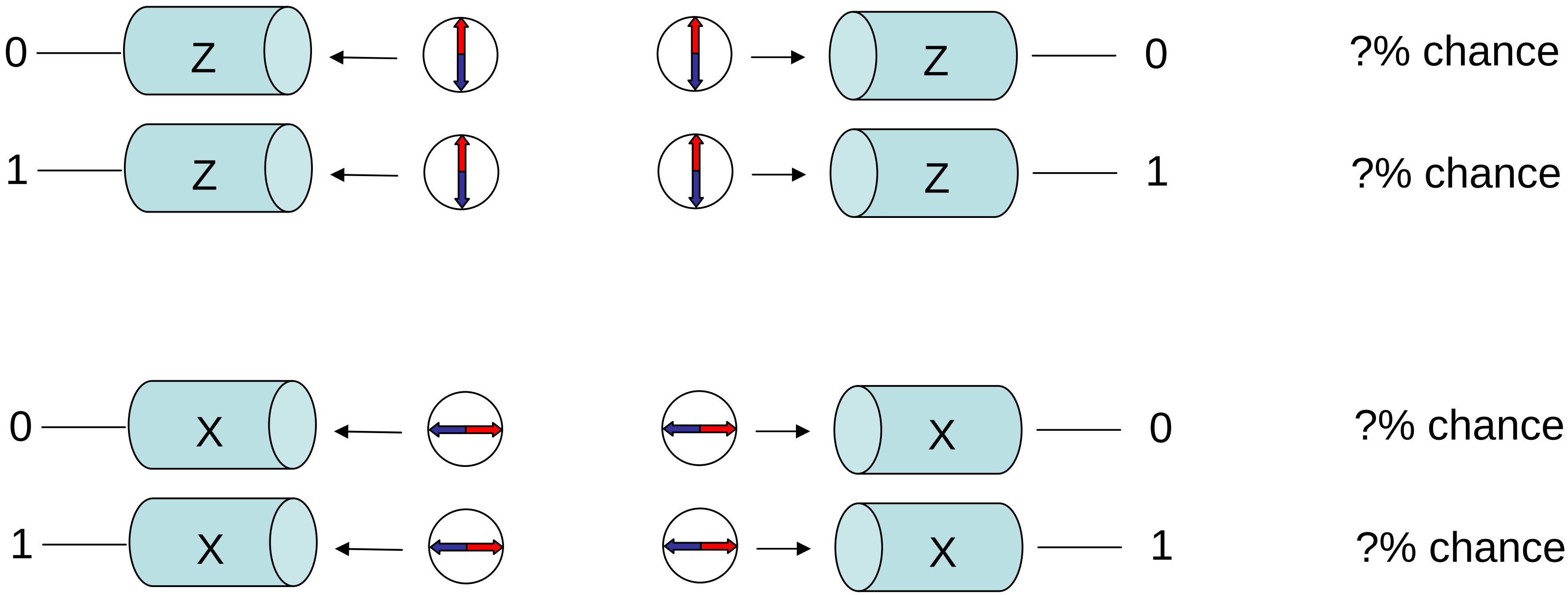
$|X = 0\rangle$
$|Z = 0\rangle$

$$X_1 + X_2 = 0$$
$$Z_1 + Z_2 = 0$$

$$|Z_1 = Z_2, X_1 = X_2\rangle$$

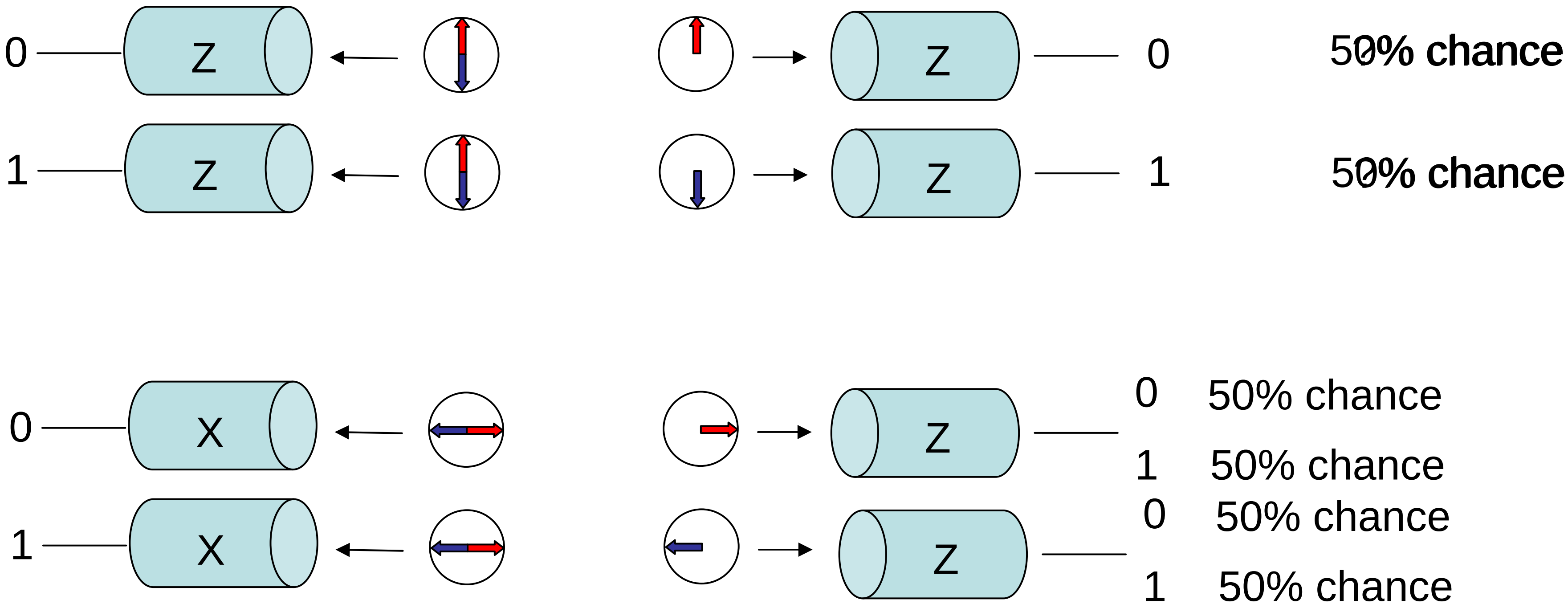
Quantum mechanics 102: Entanglement

The two qubit state $|Z_1 = Z_2, X_1 = X_2\rangle$ is called an EPR state.
(Bell state, maximally entangled state)



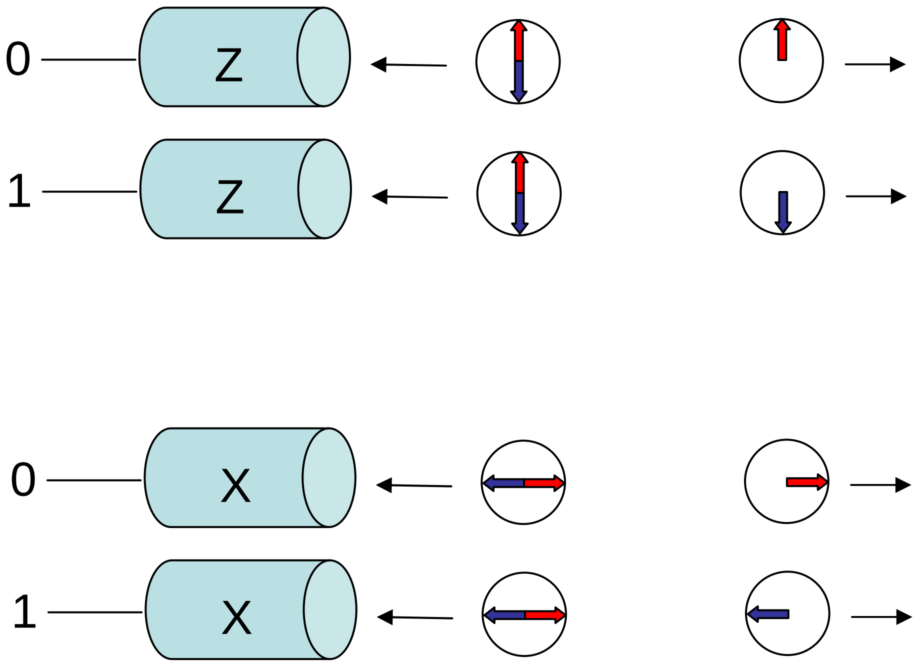
Quantum mechanics 102: Entanglement

The two qubit state $|Z_1 = Z_2, X_1 = X_2\rangle$ is called an EPR state.
(Bell state, maximally entangled state)



Quantum mechanics 102: Entanglement

The two qubit state $|Z_1 = Z_2, X_1 = X_2\rangle$ is called an EPR state.
(Bell state, maximally entangled state)

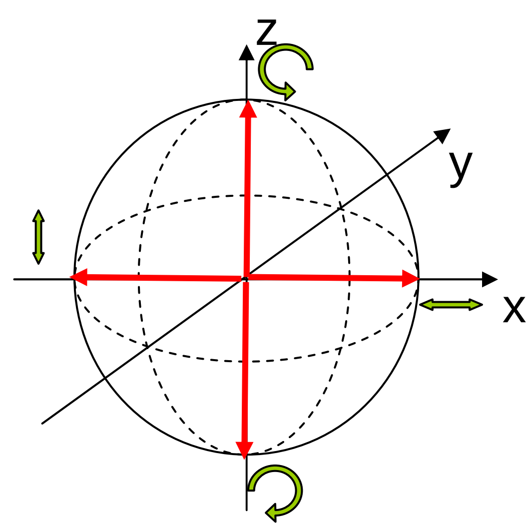


50% chance

50% chance

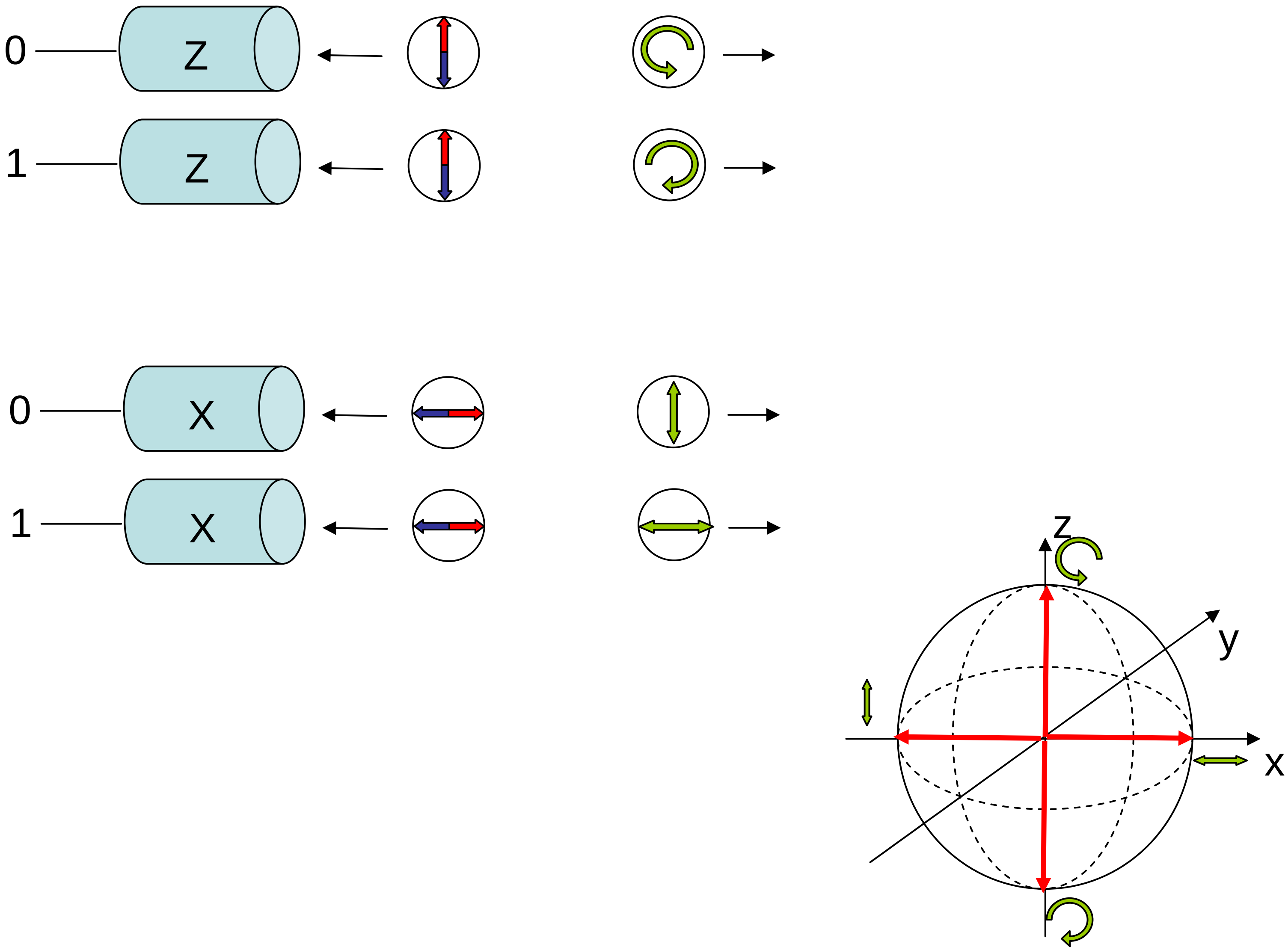
50% chance

50% chance



Quantum mechanics 102: Entanglement

The two qubit state $|Z_1 = Z_2, X_1 = X_2\rangle$ is called an EPR state.
(Bell state, maximally entangled state)



50% chance

50% chance

50% chance

50% chance

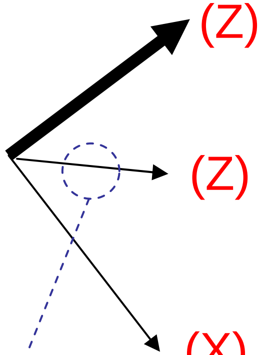
BB84 protocol

Net key gain: $N(1-h_X-h_Z)$

Encrypted communication of Nh_Z bits
to correct Bob's sifted key to match with Alice's.

Z sifted key $\xrightarrow{\text{error correction}}$ reconciled key $\xrightarrow{\text{privacy amplification}}$ final key

N bits → N bits → $N(1-h_X)$ bits

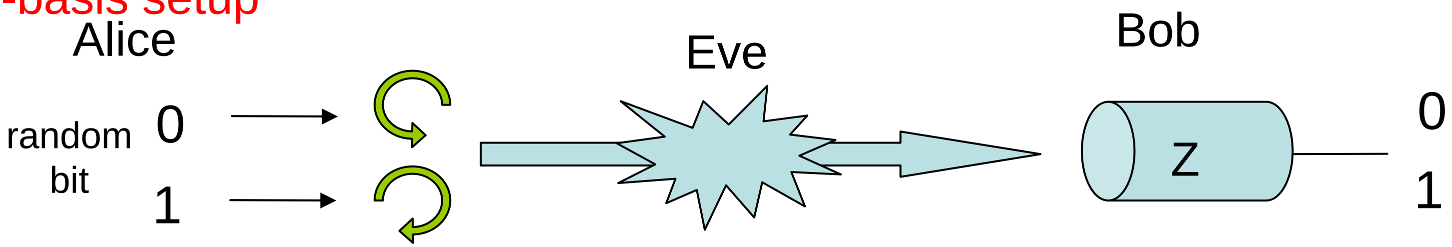


Compare the bit values to observe the error rate ϵ_Z

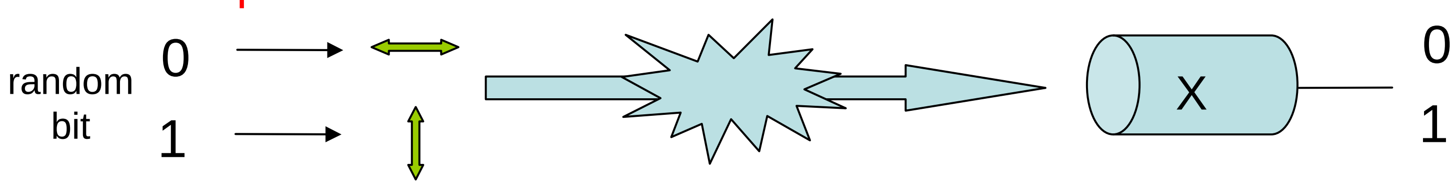
Compare the bit values to observe the error rate ϵ_X

Fair sampling
(No control from Eve)

Z-basis setup



X-basis setup

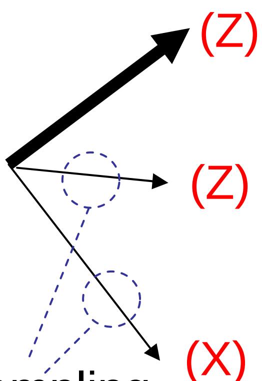


BB84 protocol

Net key gain: $N(1 - h_X - h_Z)$

Encrypted communication of Nh_Z bits
to correct Bob's sifted key to match with Alice's.

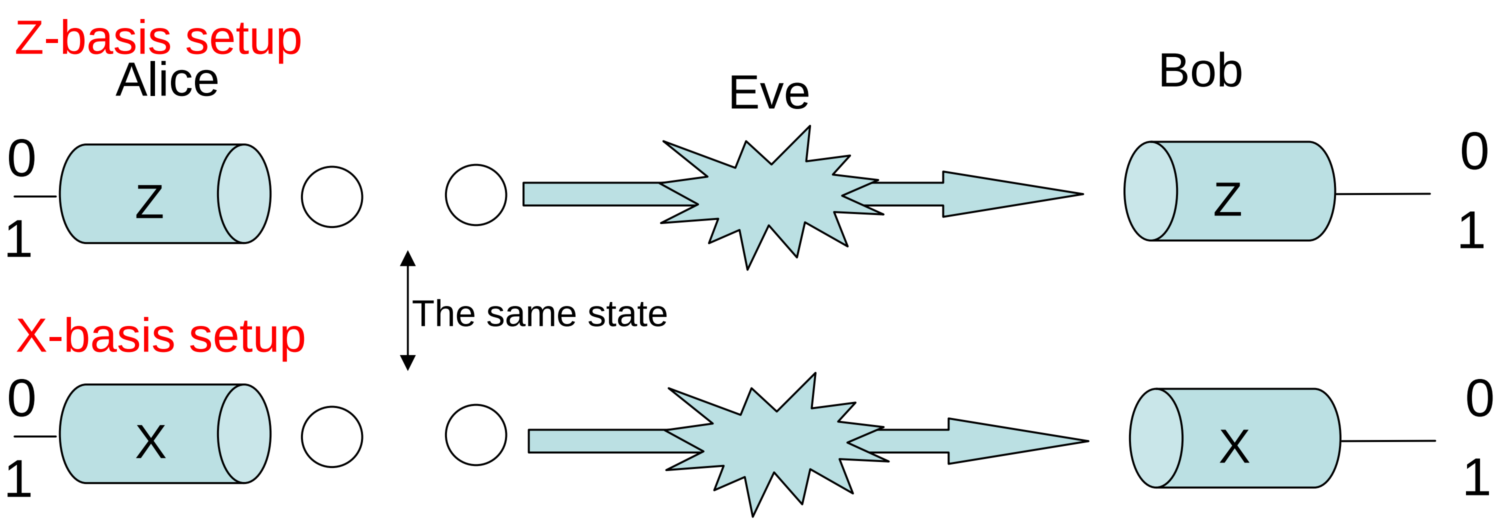
Z sifted key N bits $\xrightarrow{\text{error correction}}$ reconciled key N bits $\xrightarrow{\text{privacy amplification}}$ final key $N(1-h_X)$ bits



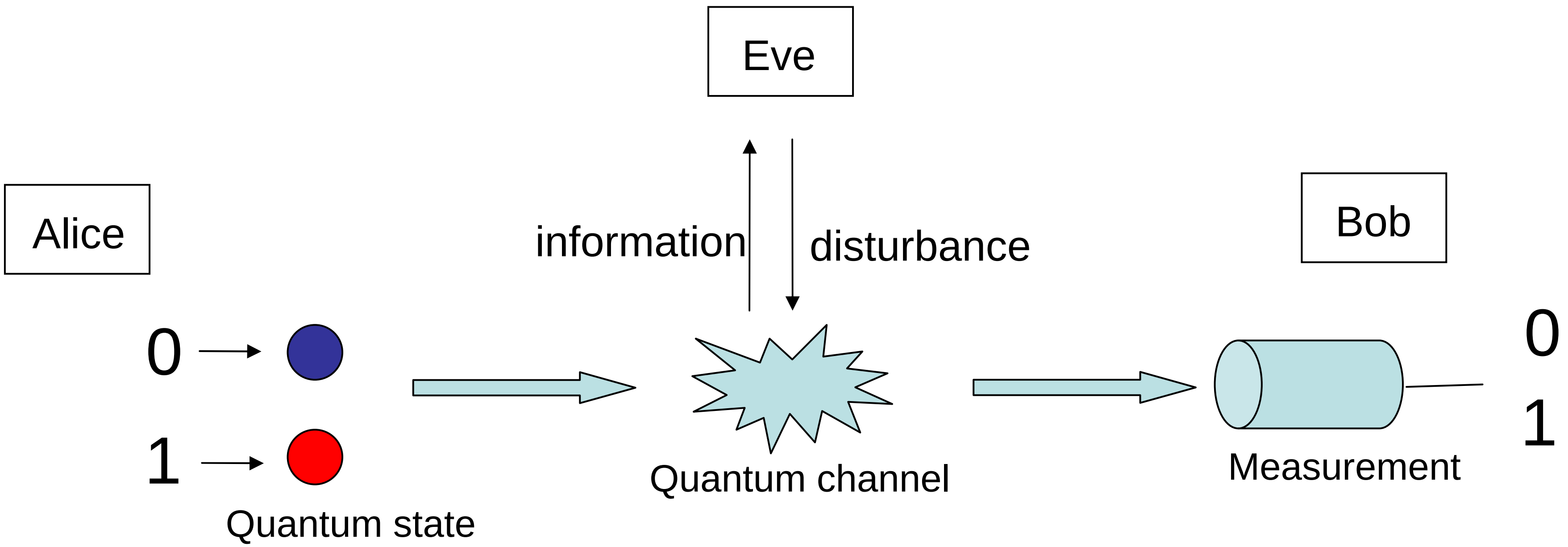
Compare the bit values to observe the error rate ϵ_Z

Compare the bit values to observe the error rate ϵ_X

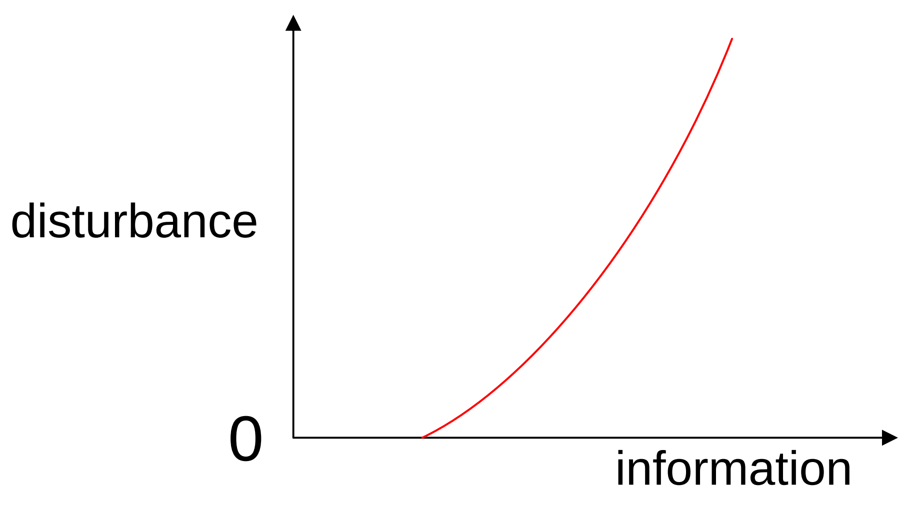
Fair sampling
(No control from Eve)



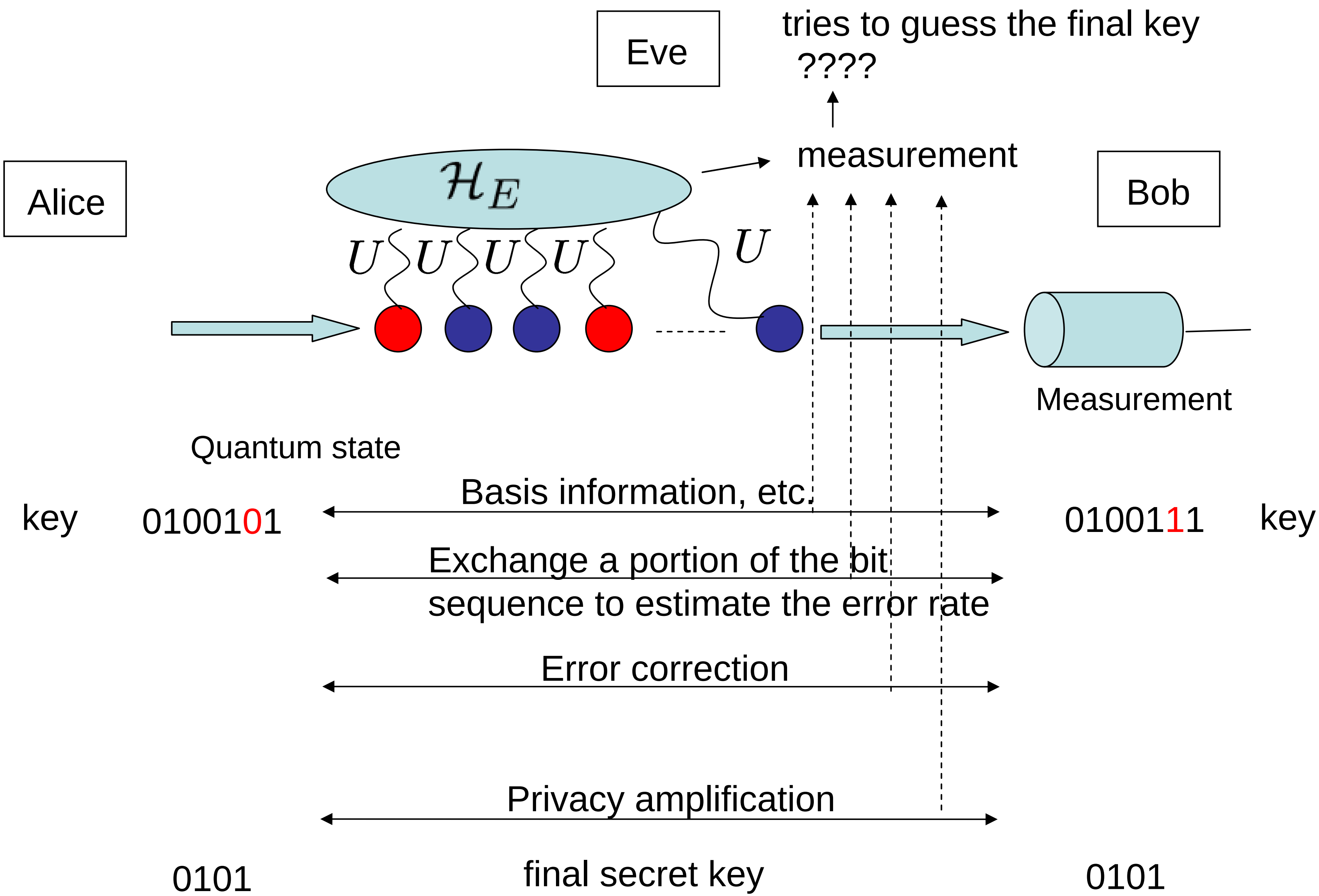
Why does QKD work?



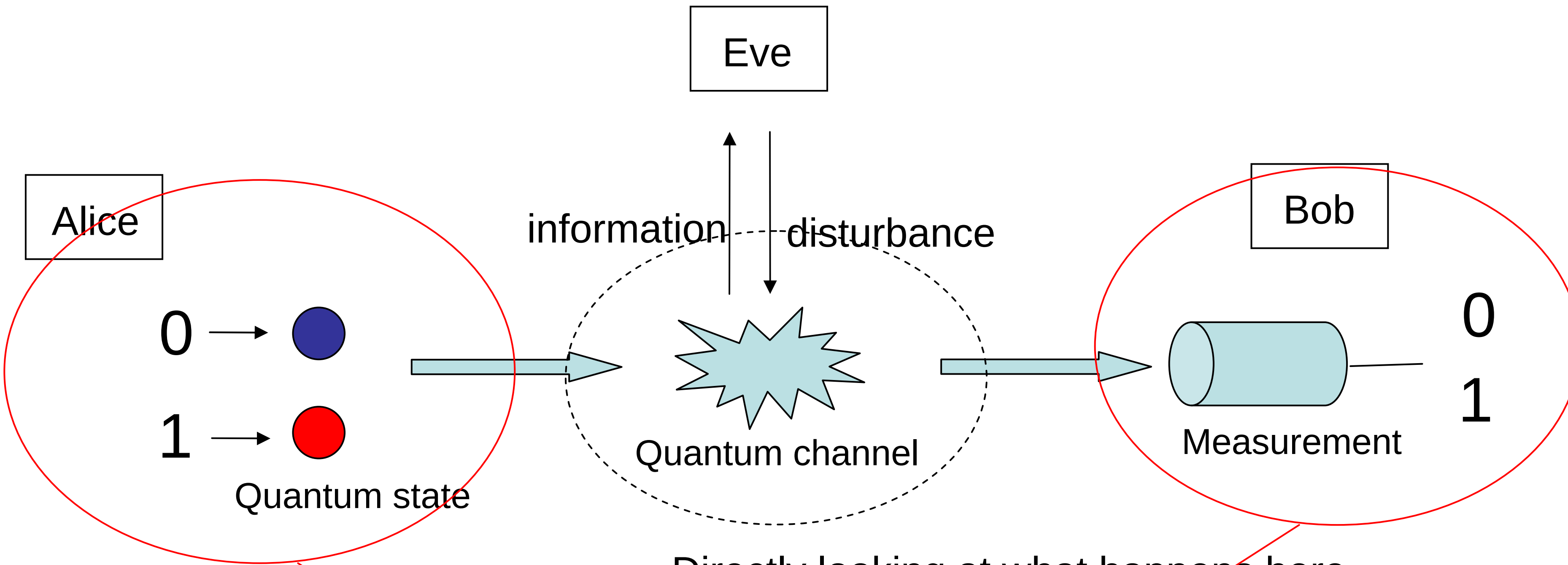
Information-disturbance trade-off



Coherent attack



How to prove the security?



Directly looking at what happens here,
is hopelessly complicated.

Many approaches to the security of QKD try to establish the security only by looking at Alice and Bob.
Relying on something testable by Alice and Bob alone.

One of such approaches —— Complementarity

Complementarity

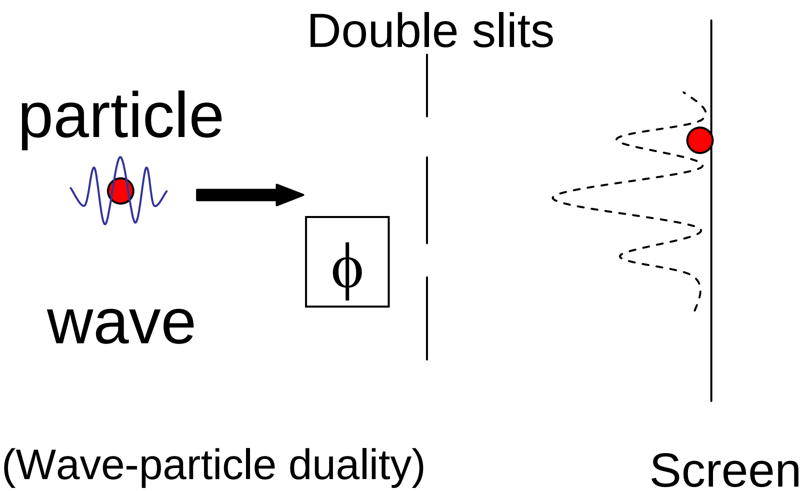
In quantum mechanics, we encounter the situation where …

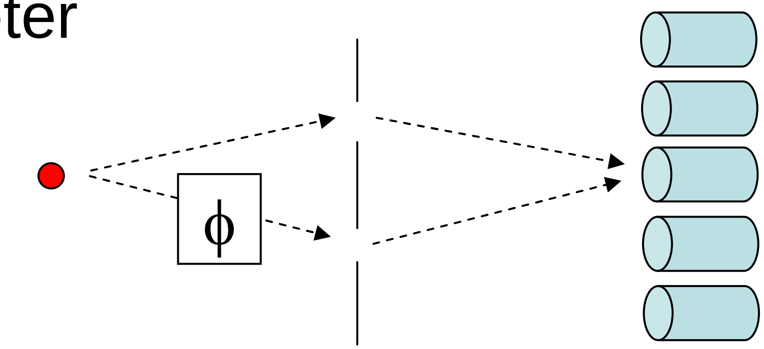
Task 1

Task 2

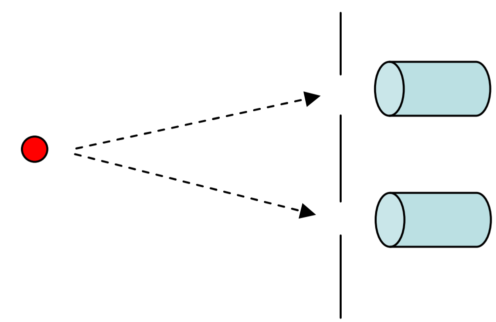
One can choose task 1 and accomplish it.
One can choose task 2 and accomplish it.
But no one can accomplish both.

Example: single-particle interferometer





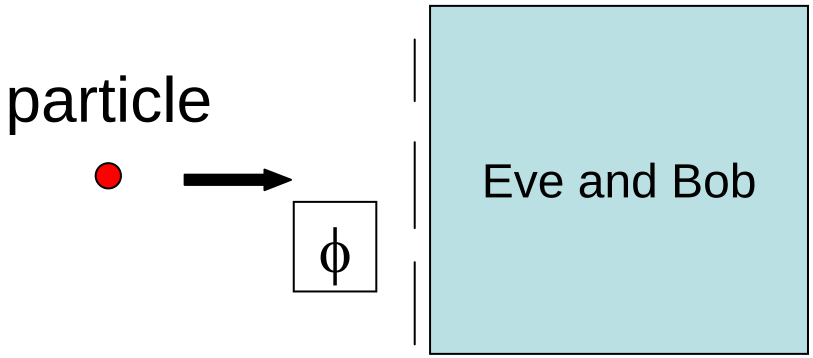
Phase information



Which-path information

One cannot obtain both types of information at the same time.

Complementarity and cryptography



Bob: I have obtained the which-path information correctly, but if I wanted, I could have obtained the phase information correctly instead.

If we can prove that Bob's claim is true, we don't have to interrogate Eve.

One cannot obtain both types of information at the same time.

⇒ Eve should have no which-path information.

Complementarity

Z-basis task

Either of the tasks is feasible.

Guess Alice’s Z-basis outcome.

X-basis task

Guess Alice’s X-basis outcome.

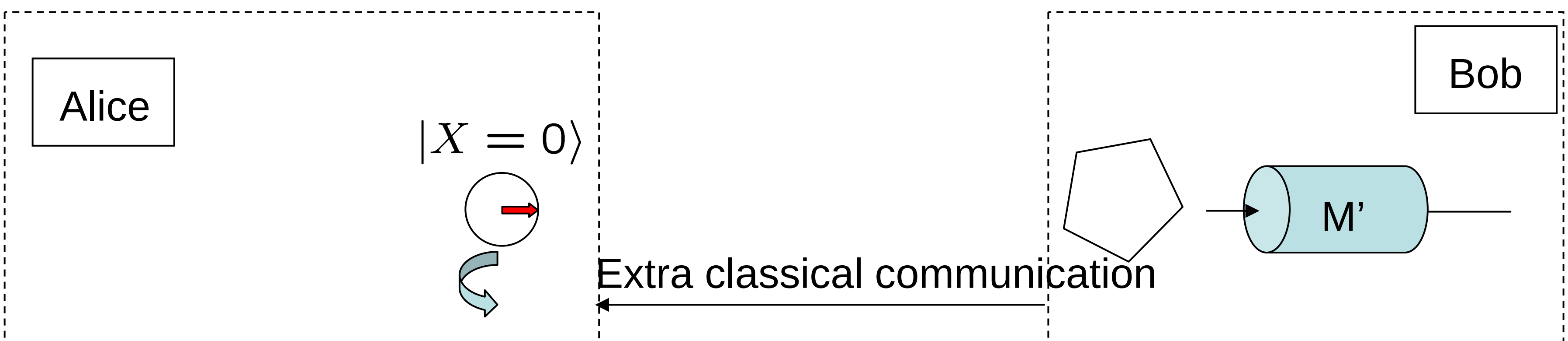
A weaker version of X task: extra classical communication

Z-basis task

Either of the tasks is feasible.

Guess Alice's Z-basis outcome.

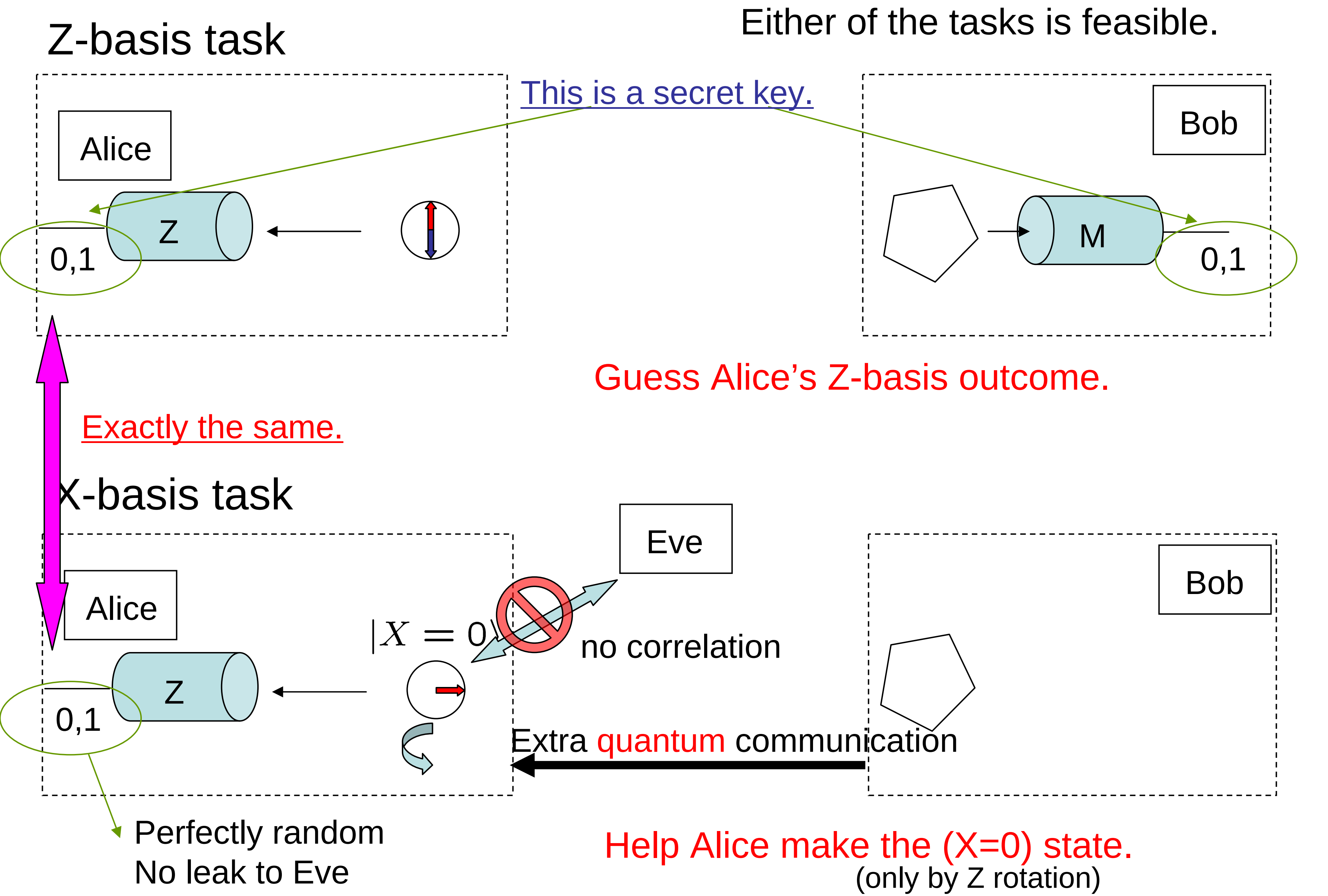
X-basis task



Help Alice make the (X=0) state.

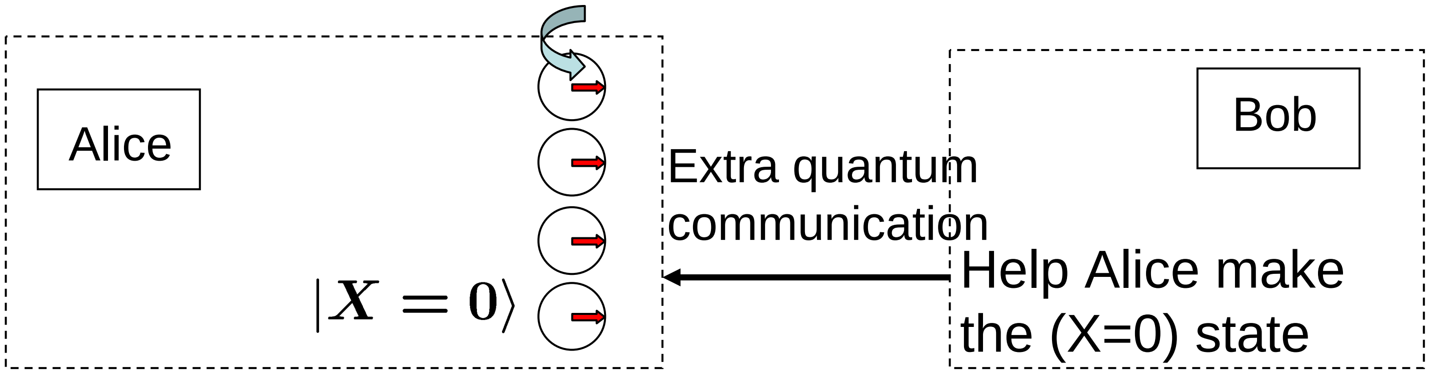
(only by Z rotation)

Feasibility of the two complementary tasks means a secret key



Feasibility of the two complementary tasks means a secret key

Z-basis task



X-basis task

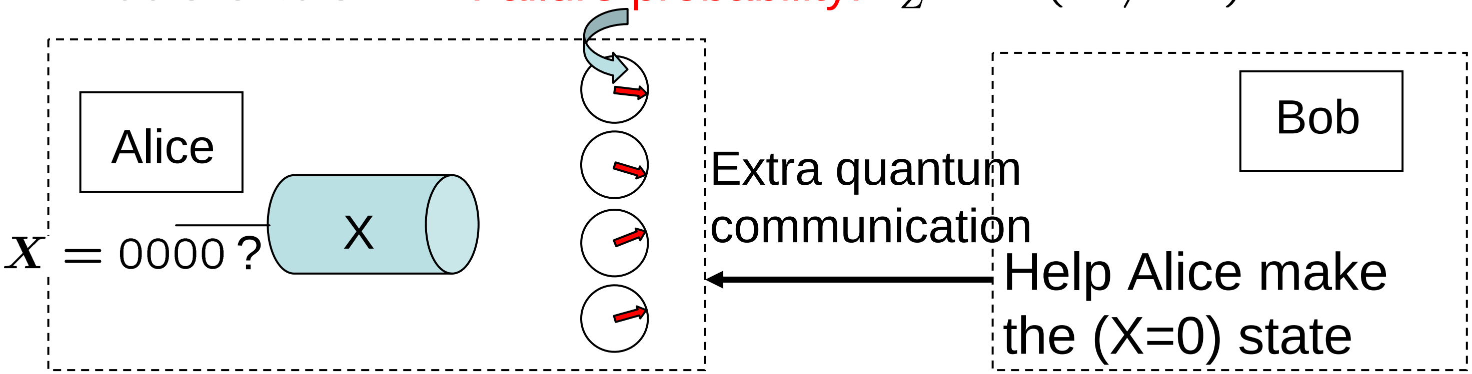
Ideal key: $\tau_{ABE} = \sum_{Z} 2^{-n} |Z, Z\rangle\langle Z, Z|_{AB} \otimes \rho_E$

- Alice's key = Bob's key
- The key is uniform
- No correlation to Eve's system

The state over the three systems:
Alice's key, Bob's key, Eve's quantum system

Effect of small imperfections

Z-basis task   Failure probability: $\delta_Z \equiv \Pr(\boldsymbol{Z} \neq \boldsymbol{Z}')$



X-basis task   Failure probability: $\delta_X \equiv \Pr(\boldsymbol{X} \neq \boldsymbol{0})$

Ideal key: $\tau_{ABE} = \sum_{\boldsymbol{Z}} 2^{-n} |\boldsymbol{Z}, \boldsymbol{Z}\rangle\langle \boldsymbol{Z}, \boldsymbol{Z}|_{AB} \otimes \rho_E$

- Alice's key = Bob's key
- The key is uniform
- No correlation to Eve's system

Final key: $\rho_{ABE} = \sum_{\boldsymbol{Z},\boldsymbol{Z}'} p_{\boldsymbol{Z},\boldsymbol{Z}'} |\boldsymbol{Z}, \boldsymbol{Z}'\rangle\langle \boldsymbol{Z}, \boldsymbol{Z}'|_{AB} \otimes \rho_E^{(\boldsymbol{Z},\boldsymbol{Z}')}$

The state over the three systems:
Alice's key, Bob's key, Eve's quantum system

Imperfection of the final key:
$\delta_{\text{key}} \equiv \|\tau_{ABE} - \rho_{ABE}\|_1$

Trace distance as a measure of distinguishability

$$\delta_{\text{key}} \equiv \|\tau_{ABE} - \rho_{ABE}\|_1$$

It never increases in any physical process χ

$$\|\tau_{ABE} - \rho_{ABE}\|_1 \geq \|\chi(\tau_{ABE}) - \chi(\rho_{ABE})\|_1$$

When the two output states can be regarded as probabilities on a classical variable,

$$\|\chi(\tau_{ABE}) - \chi(\rho_{ABE})\|_1 = \sum_x |p_\tau(x) - p_\rho(x)|$$ (Total variation distance)

This implies that, no matter what applications the final key is used for, there should be no big difference from the case where an ideal key was used instead.

Triangle inequality

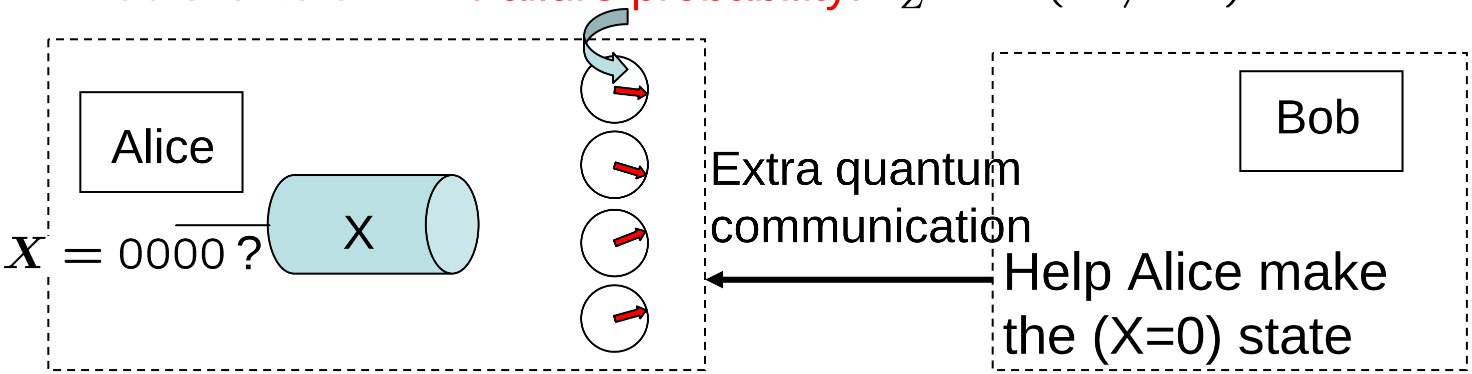
$$\|\tau - \rho\|_1 \leq \|\tau - \sigma\|_1 + \|\sigma - \rho\|_1$$

Imperfections accumulate nicely.

Effect of small imperfections

Z-basis task

Failure probability: $\delta_Z \equiv \mathrm{Pr}(Z \neq Z')$



X-basis task

Failure probability: $\delta_X \equiv \mathrm{Pr}(X \neq \mathbf{0})$

Ideal key: $\tau_{ABE} = \sum_{Z} 2^{-n} |Z, Z\rangle\langle Z, Z|_{AB} \otimes \rho_E$

- Alice's key = Bob's key
- The key is uniform
- No correlation to Eve's system

Final key: $\rho_{ABE} = \sum_{Z, Z'} p_{Z,Z'} |Z, Z'\rangle\langle Z, Z'|_{AB} \otimes \rho_E^{(Z,Z')}$

Imperfection of the final key: $\delta_{\mathrm{key}} \equiv \|\tau_{ABE} - \rho_{ABE}\|_1$

Security proof via complementarity: Recipe

Find an equivalent description of the actual QKD protocol, such that the final key is directly obtained by Z-measurement on qubits.

In the actual protocol, Bob tries to learn the final key with failure probability δ_Z

Consider a virtual protocol in which Alice and Bob cooperate freely to drive the qubits into the (X=0) state via Z rotations.

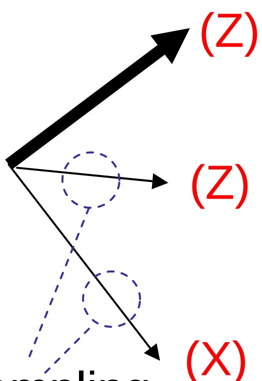
Calculate the failure probability δ_X of this protocol.

Imperfection of the final key: $\delta_{\text{key}} \equiv \|\tau_{ABE} - \rho_{ABE}\|_1 \leq 2\delta_Z + 2\sqrt{\delta_X}$

BB84 protocol

Net key gain: $N(1-h_X-h_Z)$

Encrypted communication of Nh_Z bits
to correct Bob's sifted key to match with Alice's.

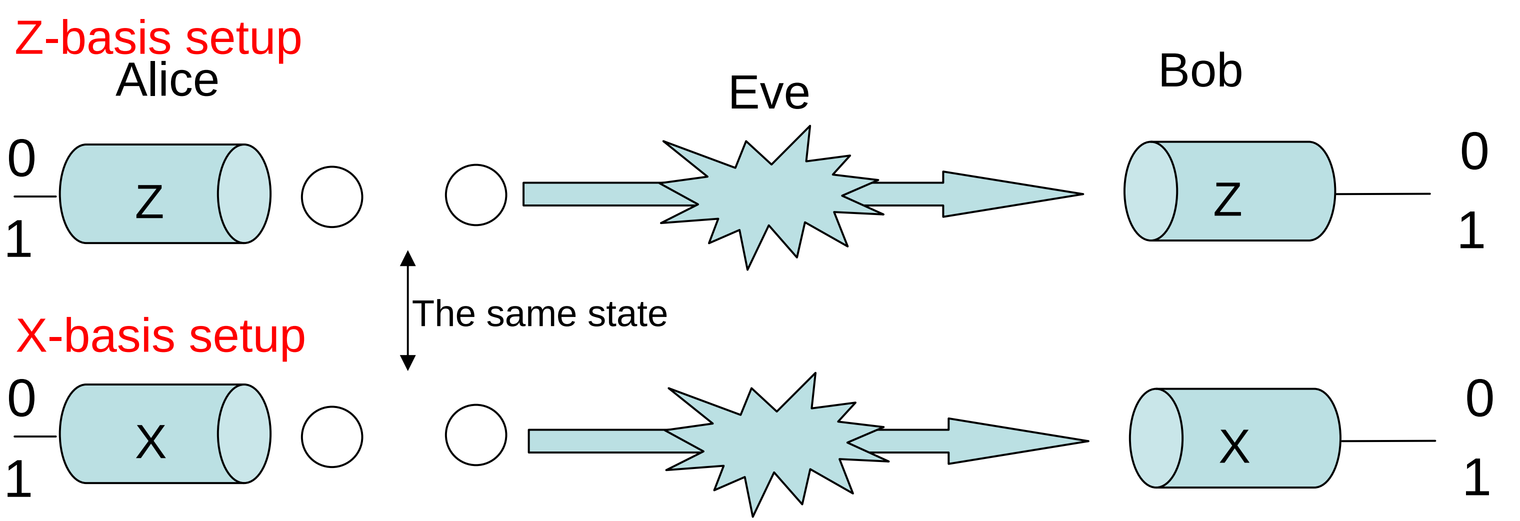


Z sifted key N bits $\xrightarrow{\text{error correction}}$ reconciled key N bits $\xrightarrow{\text{privacy amplification}}$ final key $N(1-h_X)$ bits

Compare the bit values to observe the error rate ϵ_Z

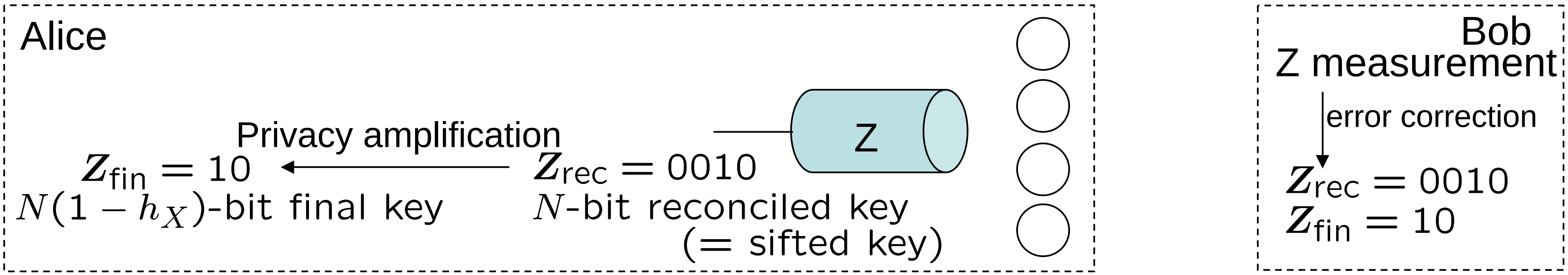
Compare the bit values to observe the error rate ϵ_X

Fair sampling
(No control from Eve)



Regarding the final key as the Z-measurement outcome

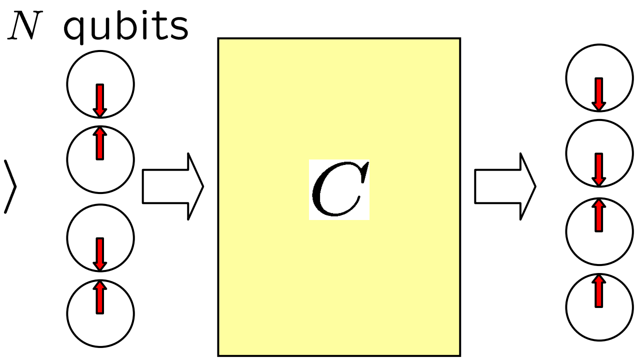
Privacy amplification: Apply random $(N \times N)$ invertible binary matrix C, and adopt the first $N(1-h_X)$ bits.



QKD protocol

Quantum mechanics 102: Interaction among qubits

$|\boldsymbol{Z} = \boldsymbol{z}\rangle$



$|\boldsymbol{Z} = \boldsymbol{z}C\rangle$

$C : (N \times N)$ invertible binary matrix

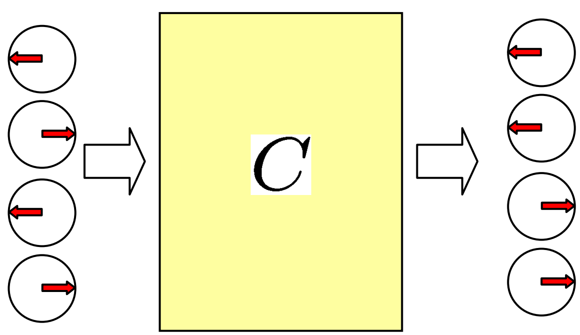
Reversible linear transformation of Z value

FACT:

For any C, there exists such a physical operation that is reversible, and also satisfies

...

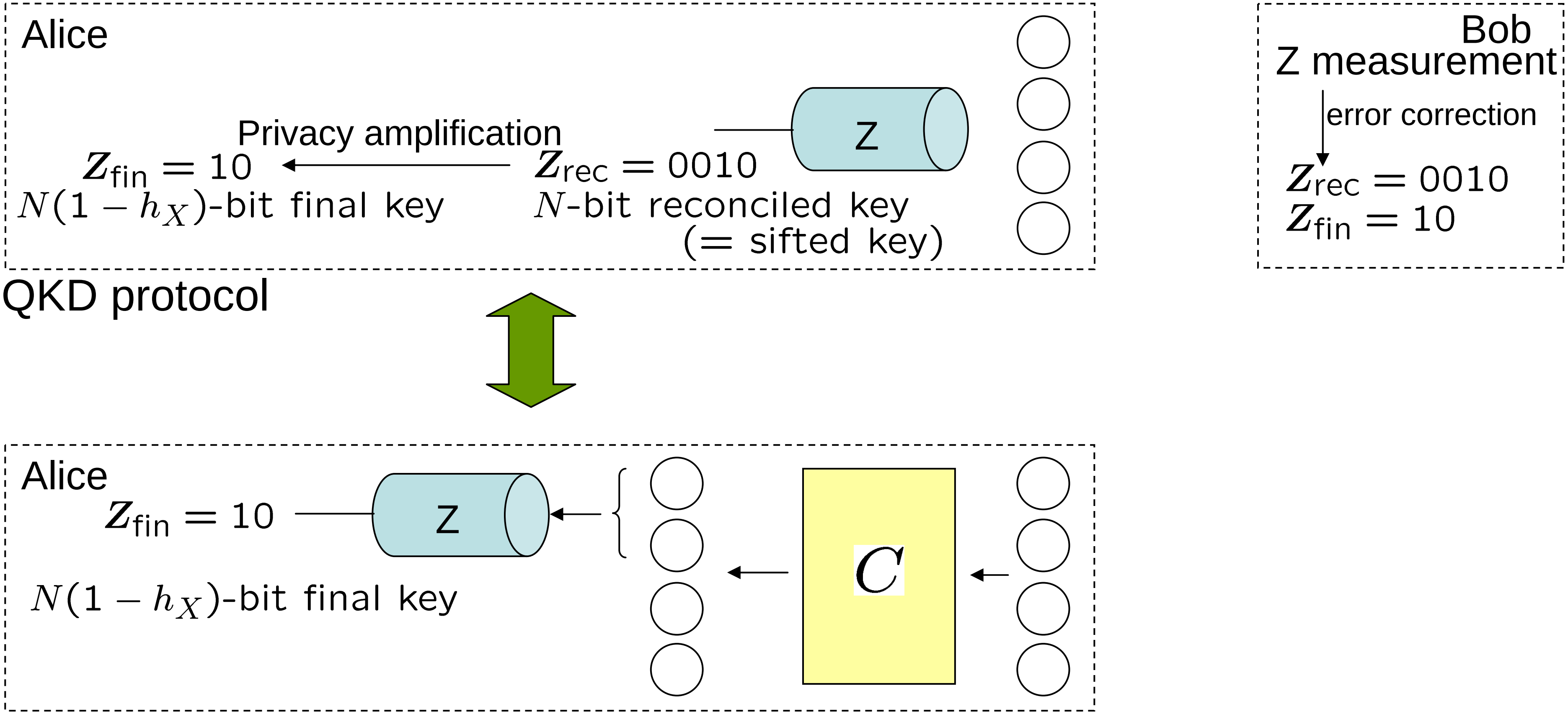
$|\boldsymbol{X} = \boldsymbol{x}\rangle$



$|\boldsymbol{X} = \boldsymbol{x}(C^{-1})^T\rangle$

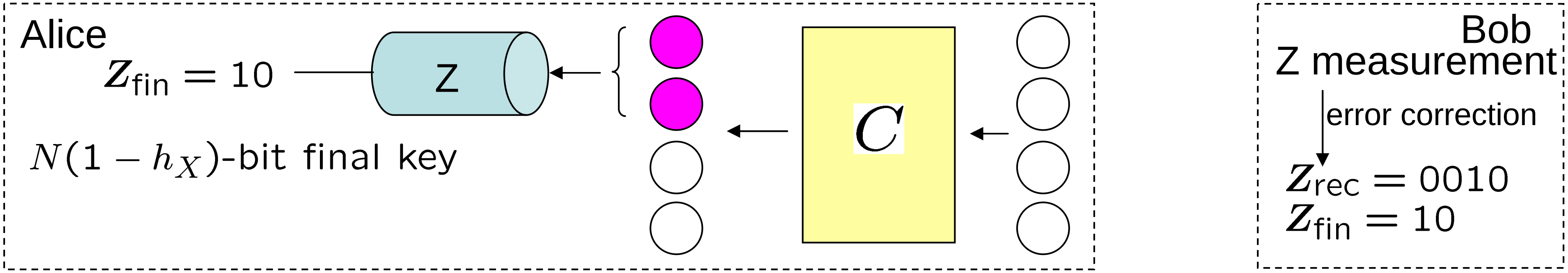
Regarding the final key as the Z-measurement outcome

Privacy amplification: Apply random $(N \times N)$ invertible binary matrix C, and adopt the first $N(1-h_X)$ bits.

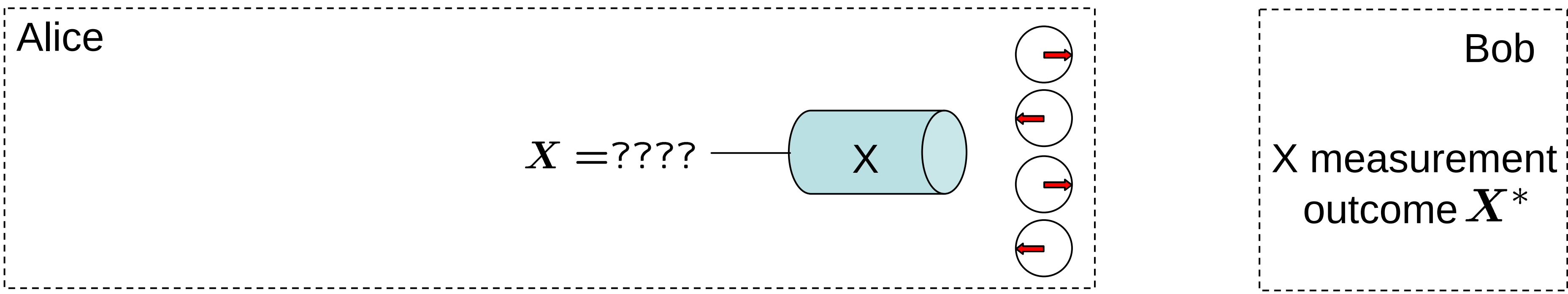


Constructing a virtual protocol

Privacy amplification: Apply random $(N \times N)$ invertible binary matrix C, and adopt the first $N(1-h_X)$ bits.



QKD protocol



A virtual protocol

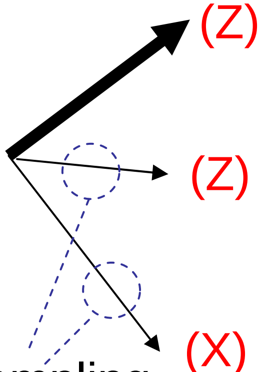
Bob provides a candidate X^*

BB84 protocol

Net key gain: $N(1-h_X-h_Z)$

Encrypted communication of Nh_Z bits
to correct Bob's sifted key to match with Alice's.

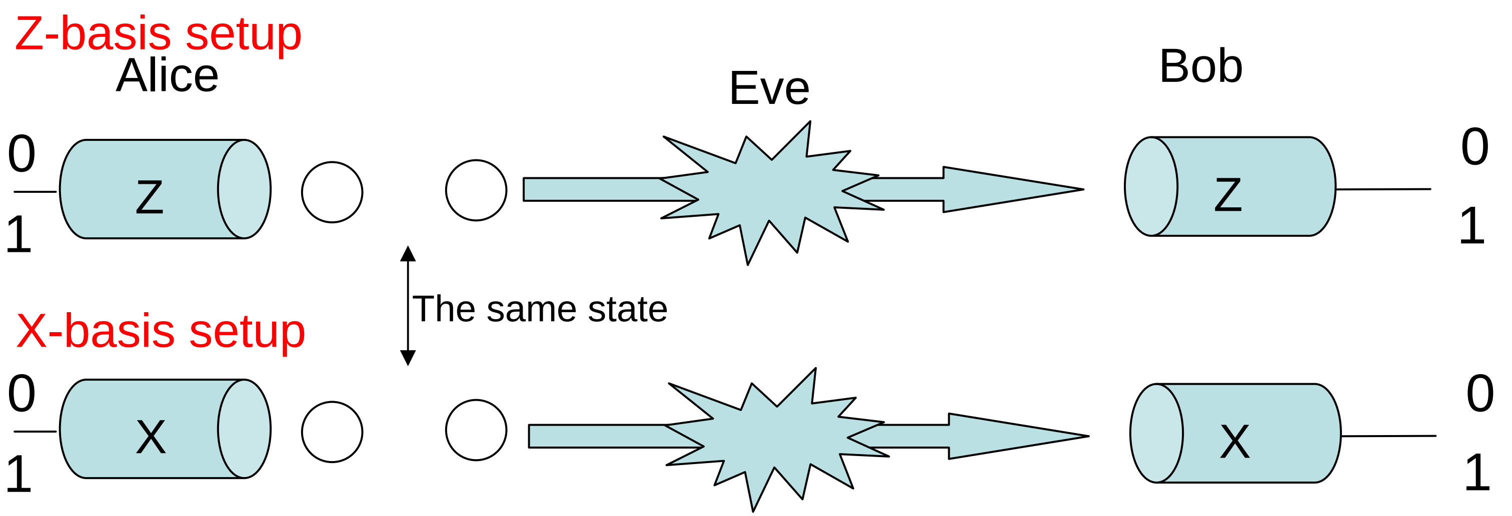
Z sifted key N bits $\xrightarrow{\text{error correction}}$ reconciled key N bits $\xrightarrow{\text{privacy amplification}}$ final key $N(1-h_X)$ bits



Compare the bit values to observe the error rate ϵ_Z

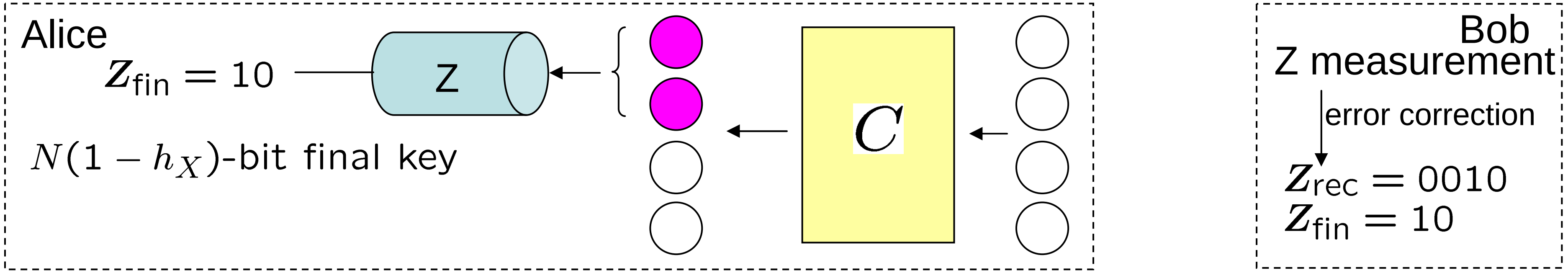
Compare the bit values to observe the error rate ϵ_X

Fair sampling
(No control from Eve)

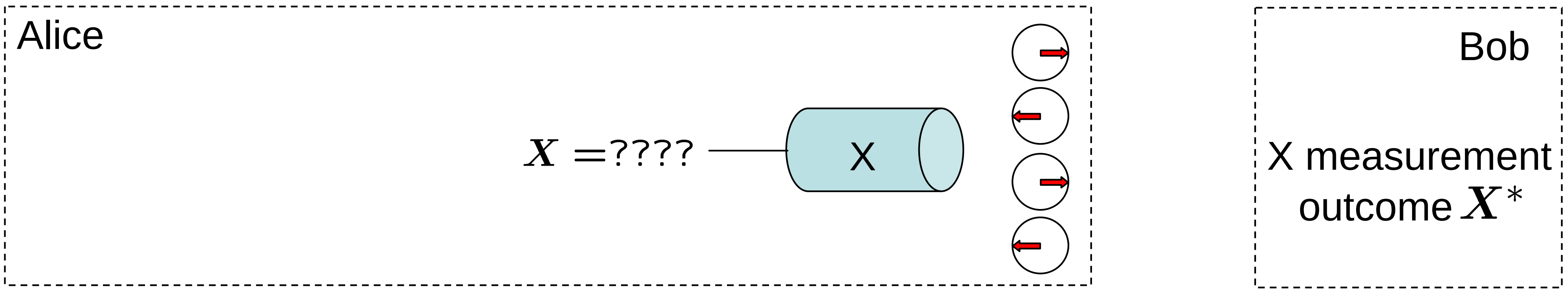


Constructing a virtual protocol

Privacy amplification: Apply random $(N \times N)$ invertible binary matrix C, and adopt the first $N(1-h_X)$ bits.



QKD protocol



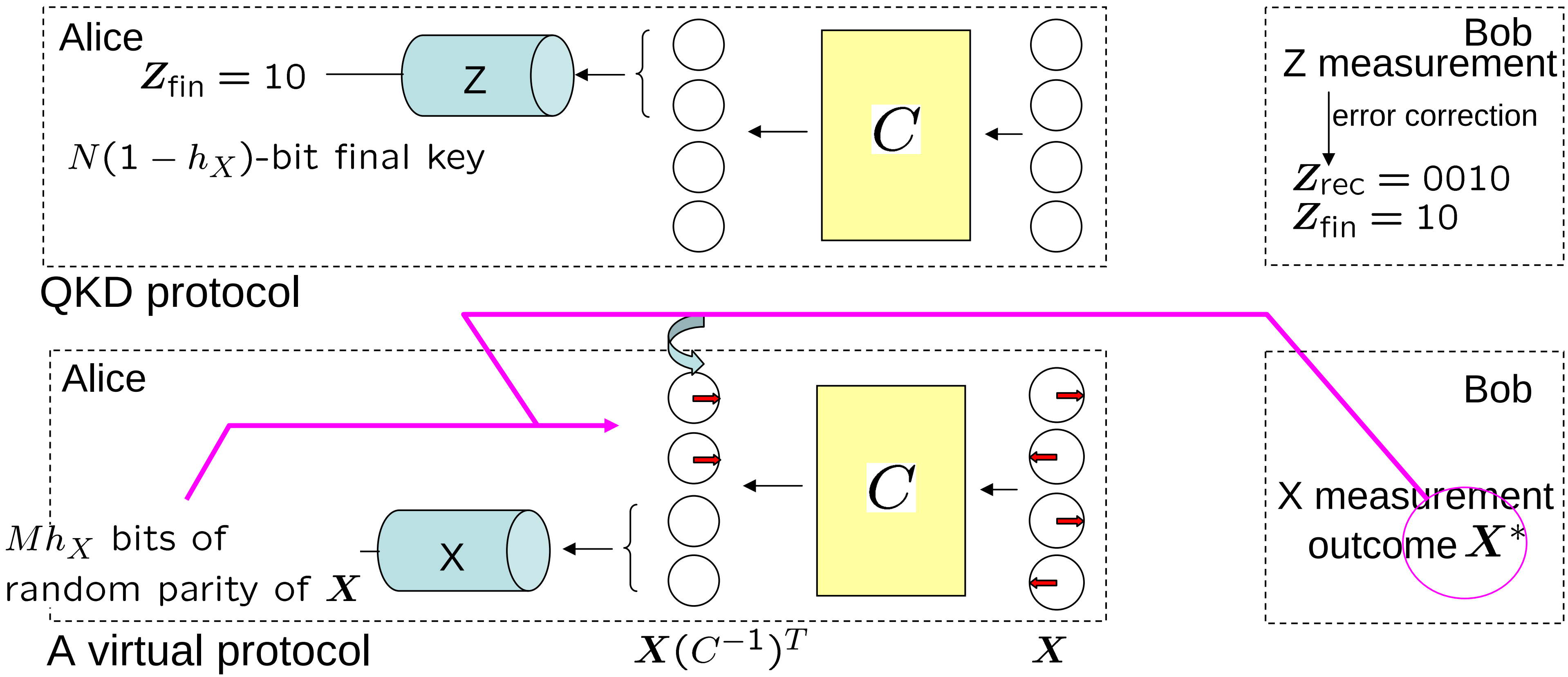
A virtual protocol

Bob provides a candidate X^*

(The random sampling test gives the error rate ϵ_X)

Constructing a virtual protocol

Privacy amplification: Apply random $(N \times N)$ invertible binary matrix C, and adopt the first $N(1-h_X)$ bits.



Bob provides a candidate X^*

(The random sampling test gives the error rate ϵ_X)

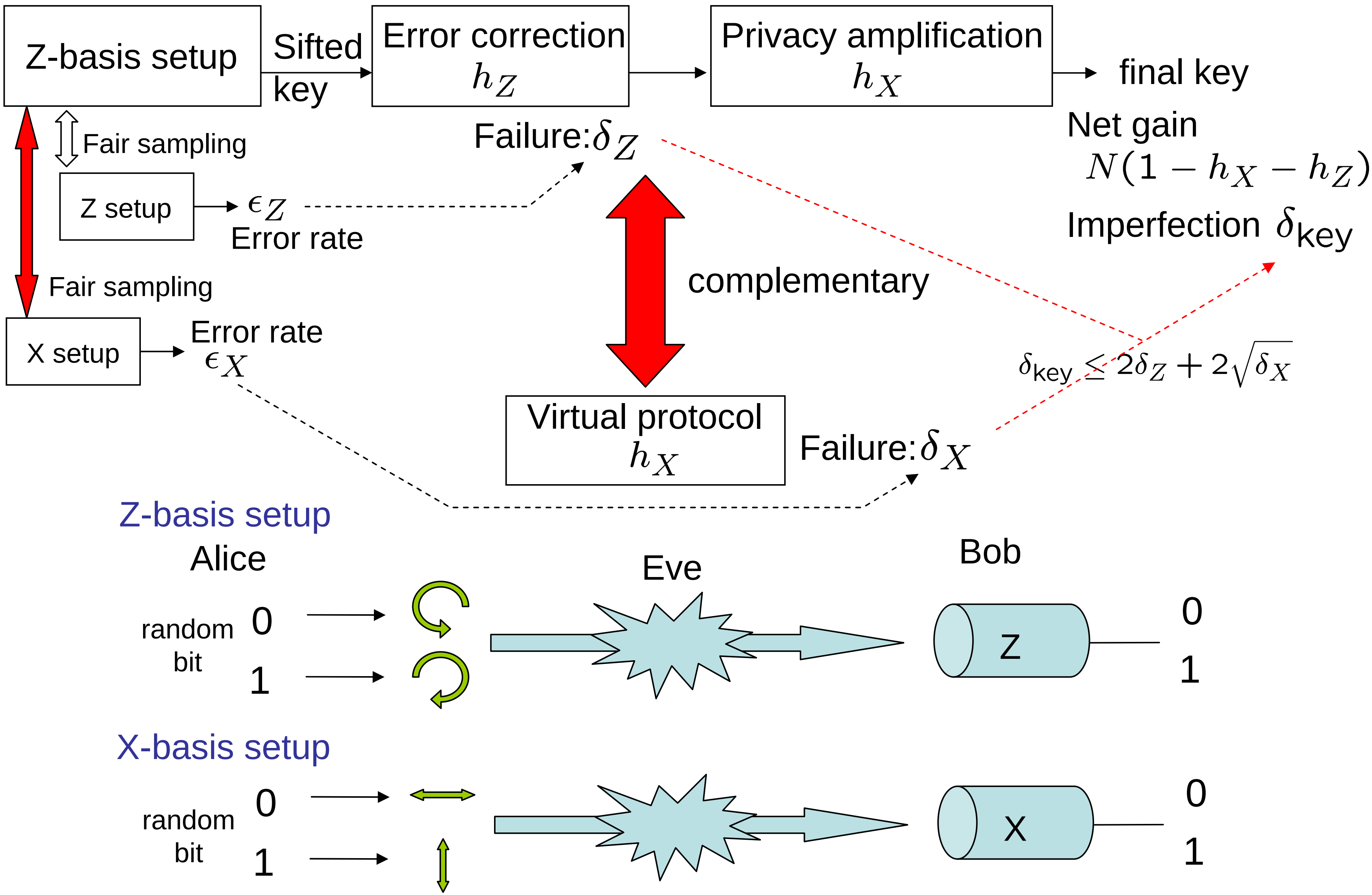
The last Nh_X bits of $X(C^{-1})^T$ are given

Guess X

$\delta_X \sim 0$ for $h_X \sim H(\epsilon_X)$

Failure probability: δ_X

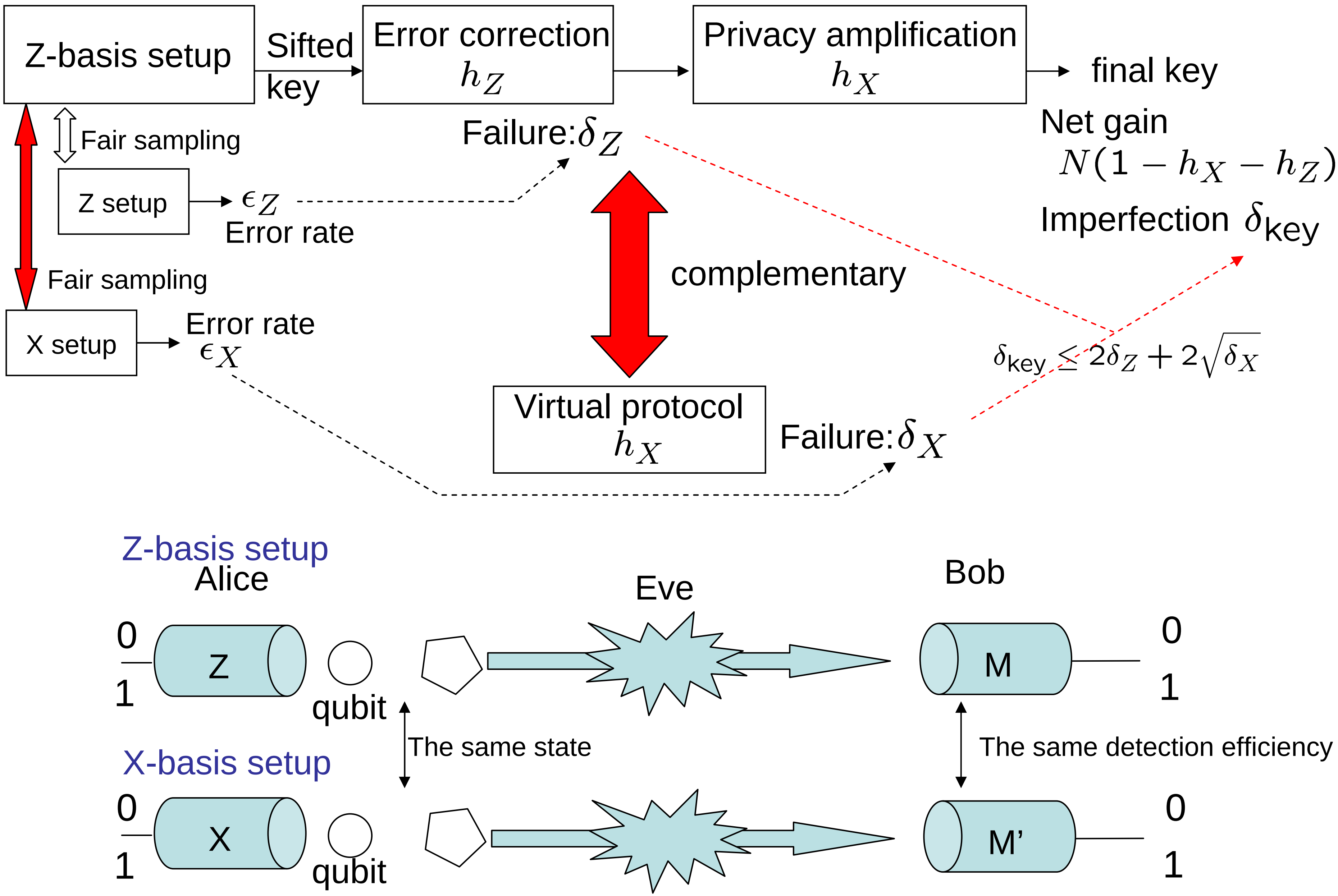
Summary: Security of BB84 protocol from complementarity



$\delta_{\text{key}} \sim 0$ for $h_X \sim H(\epsilon_X)$ and $h_Z \sim H(\epsilon_Z)$

[KP03,K.09]

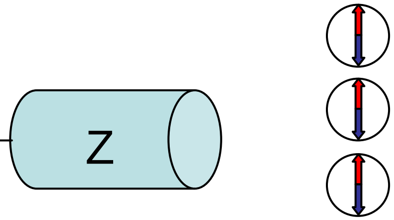
Assumptions on Alice's and Bob's devices



QKD and complementarity

Alice

$Z = 001$



Bob

$Z' = 001$

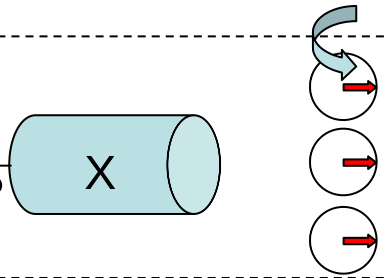
Guess Alice's
n-bit Z-basis outcome.

Z-basis task

Failure probability: $\delta_Z \equiv \Pr(Z \neq Z')$

Alice

$X = 000$?



Extra quantum communication

Bob

Help Alice make
the (X=0) state.

X-basis task

Failure probability: $\delta_X \equiv \Pr(X \neq \mathbf{0})$

Secret key can be extracted with imperfection

$$\delta_{\text{key}} \equiv \|\tau_{ABE} - \rho_{ABE}\|_1 \leq 2\delta_Z + 2\sqrt{\delta_X}$$

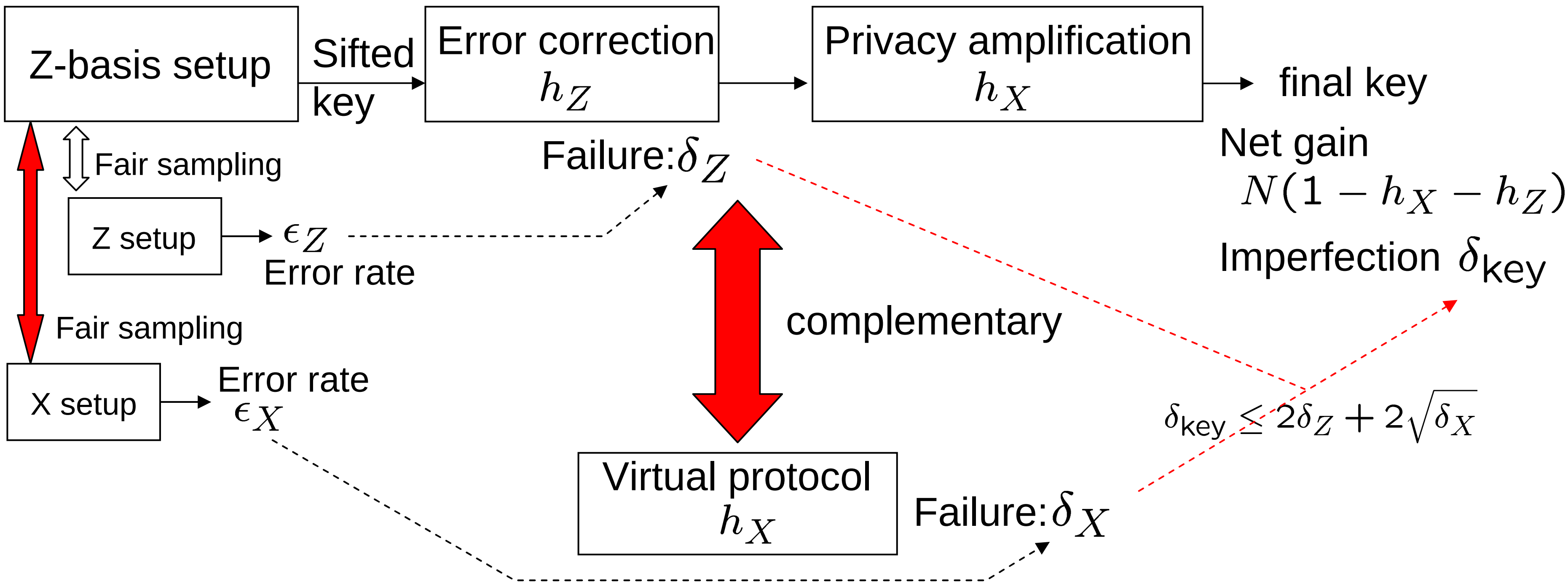
The opposite is also true. [K., 07]

Whenever the secret key can be extracted with imperfection δ_{key} ,
the two tasks are feasible with imperfections as small as

$$\delta_Z \leq \delta_{\text{key}}/2 \text{ and } \delta_X \leq \delta_{\text{key}} - (\delta_{\text{key}}/2)^2.$$

→ The complementarity approach is, in principle, applicable to any QKD scheme.

Summary



The approach based on complementarty in quantum mechanics

- The feasibility of a pair of complementary tasks guarantees the security.
- Only a few assumptions on the devices (especially for the detectors).
- Applicable to any QKD scheme in principle.
- Quantitative equivalence between two facades of quantum mechanics:
  Exclusive correlations (monogamy) and complementarity