

Complementarity and security of quantum key distribution

Osaka Univ. Masato Koashi

- Proving the security of QKD via complementarity
 - Basic idea
 - Small imperfections
 - A prescription for determining a secure key rate
- Merits in the complementarity approach
 - Applicability and relation to entanglement
 - Security from an operationally defined quantity
- Examples (BB84, BBM92, 6-state protocols)
- Summary

Complementarity

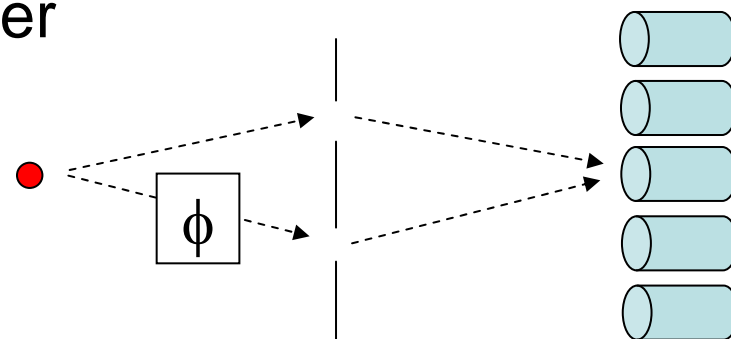
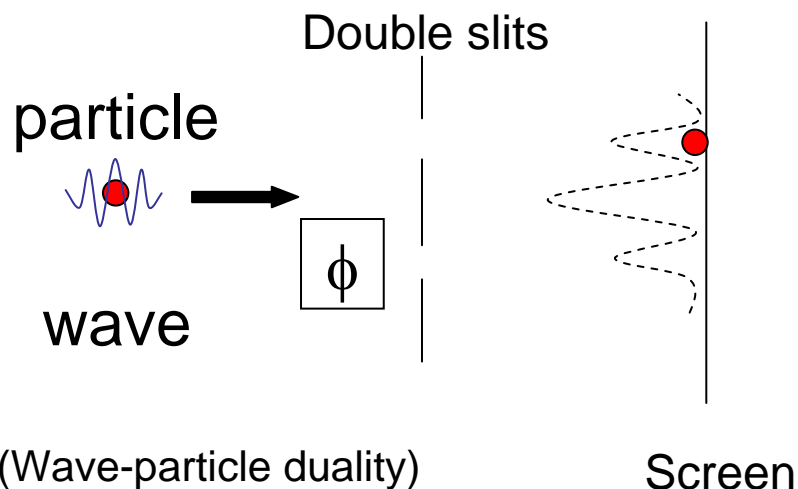
In quantum mechanics, we encounter the situation where ...

Task 1

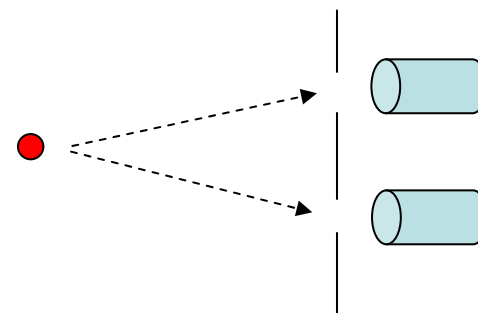
Task 2

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

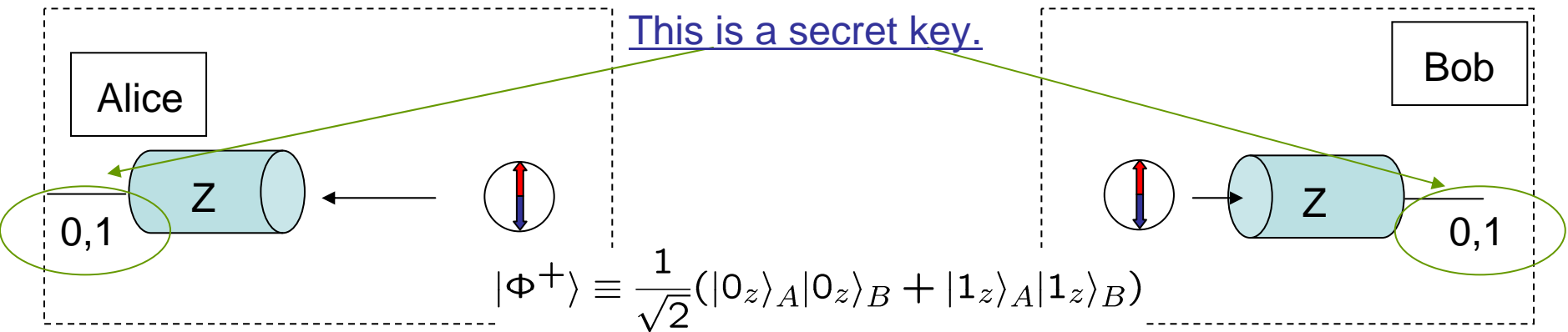


Which-path information

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

Secret key from an EPR pair of qubits

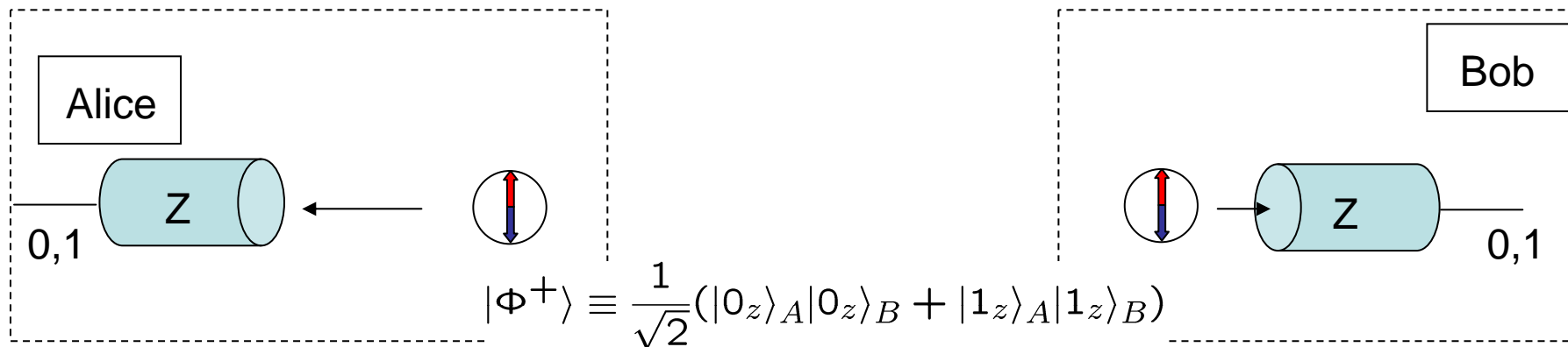
Lo & Chau (2001).



A **pure** state with an **equal** superposition of 0 and 1.

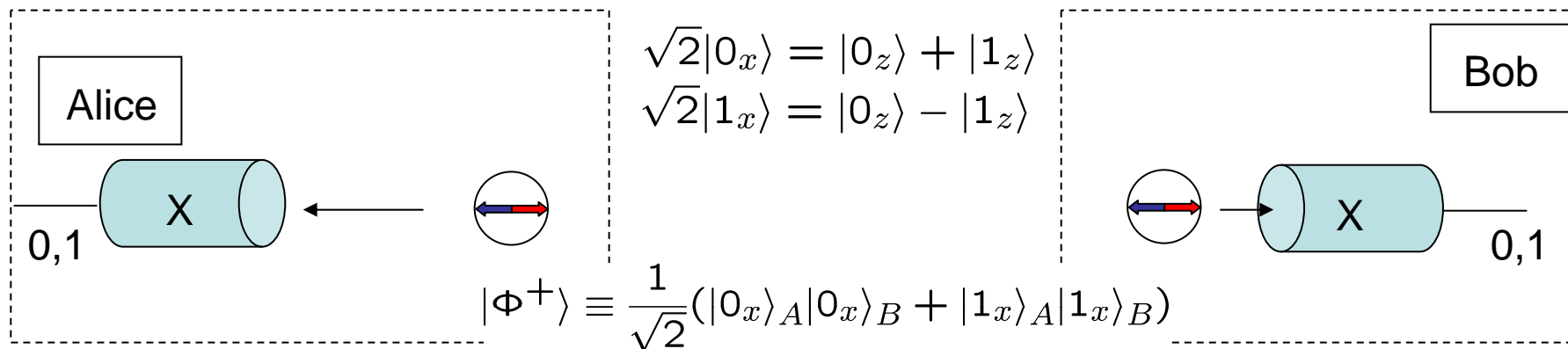
Complementarity

Z-basis task



Bob can guess Alice's Z-basis outcome.

X-basis task



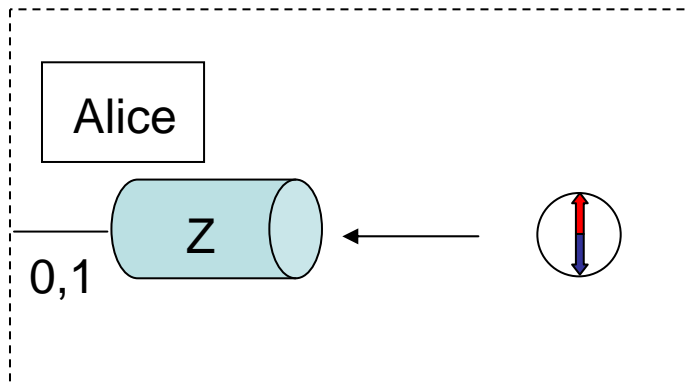
Bob can guess Alice's X-basis outcome.

Either of the tasks is feasible.

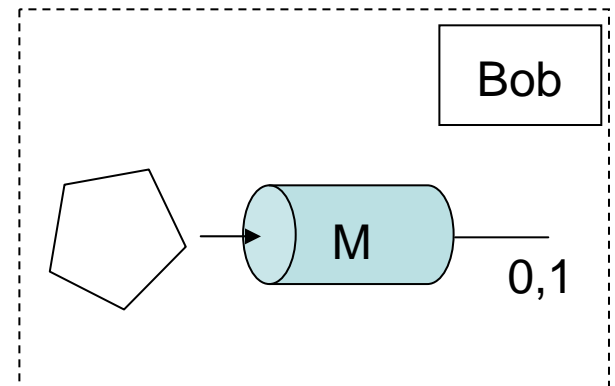
One cannot accomplish both tasks at the same time.

Complementarity

Z-basis task

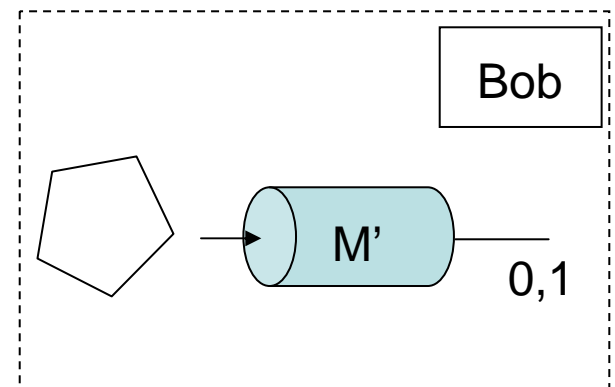
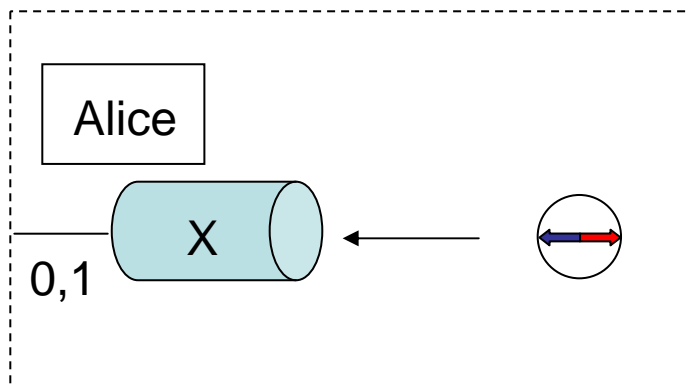


Either of the tasks is feasible.



Guess Alice's Z-basis outcome.

X-basis task

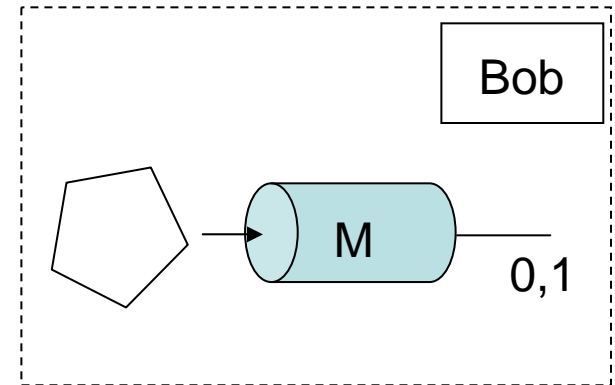
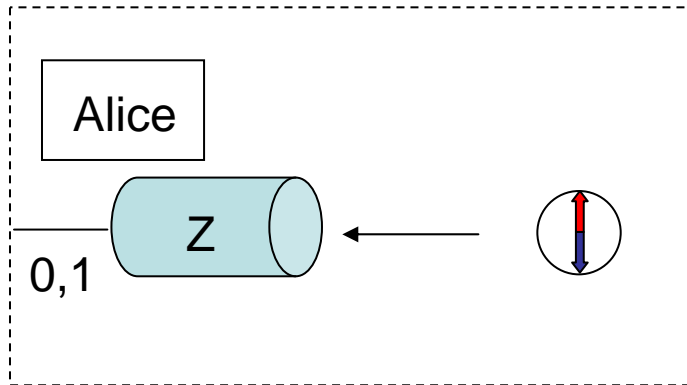


Guess Alice's X-basis outcome.

A weaker version of X task: extra classical communication

Z-basis task

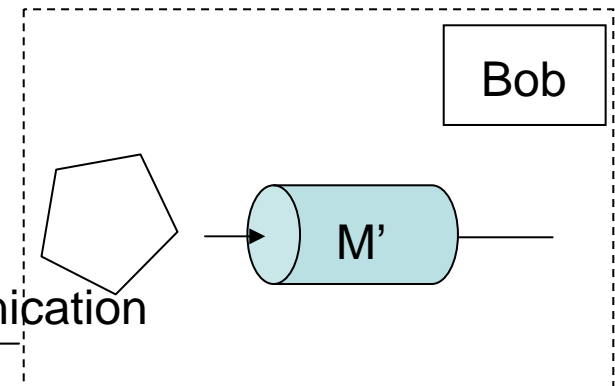
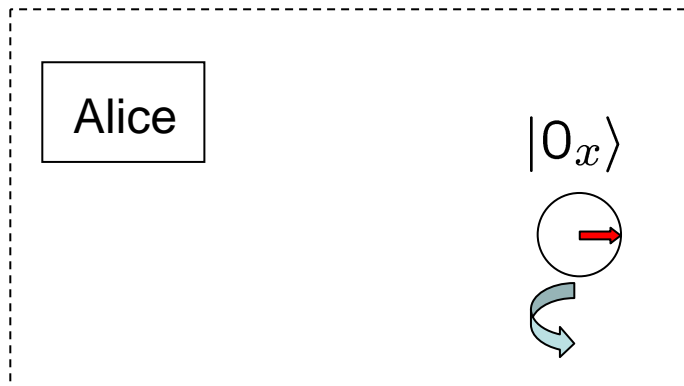
Either of the tasks is feasible.



Guess Alice's Z-basis outcome.

X-basis task

$$\begin{aligned}\sqrt{2}|0_x\rangle &= |0_z\rangle + |1_z\rangle \\ \sqrt{2}|1_x\rangle &= |0_z\rangle - |1_z\rangle\end{aligned}$$



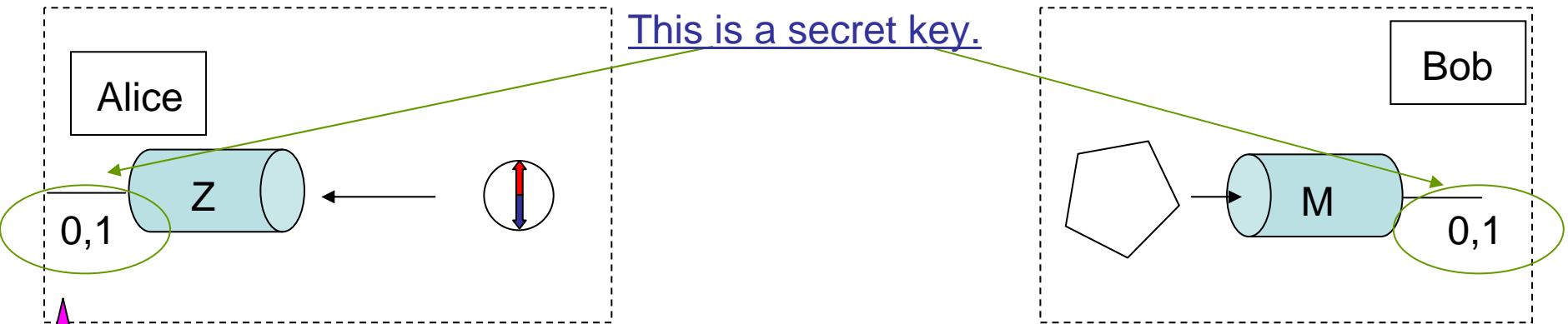
Extra classical communication

Help Alice make an X-basis eigenstate.
(without disturbing the Z-basis observable)

Feasibility of the two complementary tasks means a **secret key**

Z-basis task

Either of the tasks is feasible.

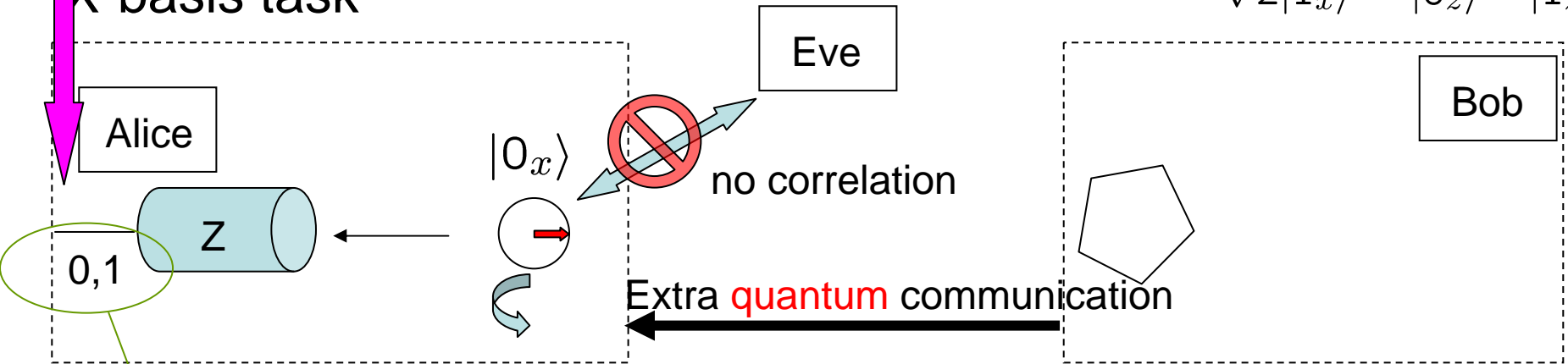


Guess Alice's Z-basis outcome.

Exactly the same.

$$\sqrt{2}|0_x\rangle = |0_z\rangle + |1_z\rangle$$
$$\sqrt{2}|1_x\rangle = |0_z\rangle - |1_z\rangle$$

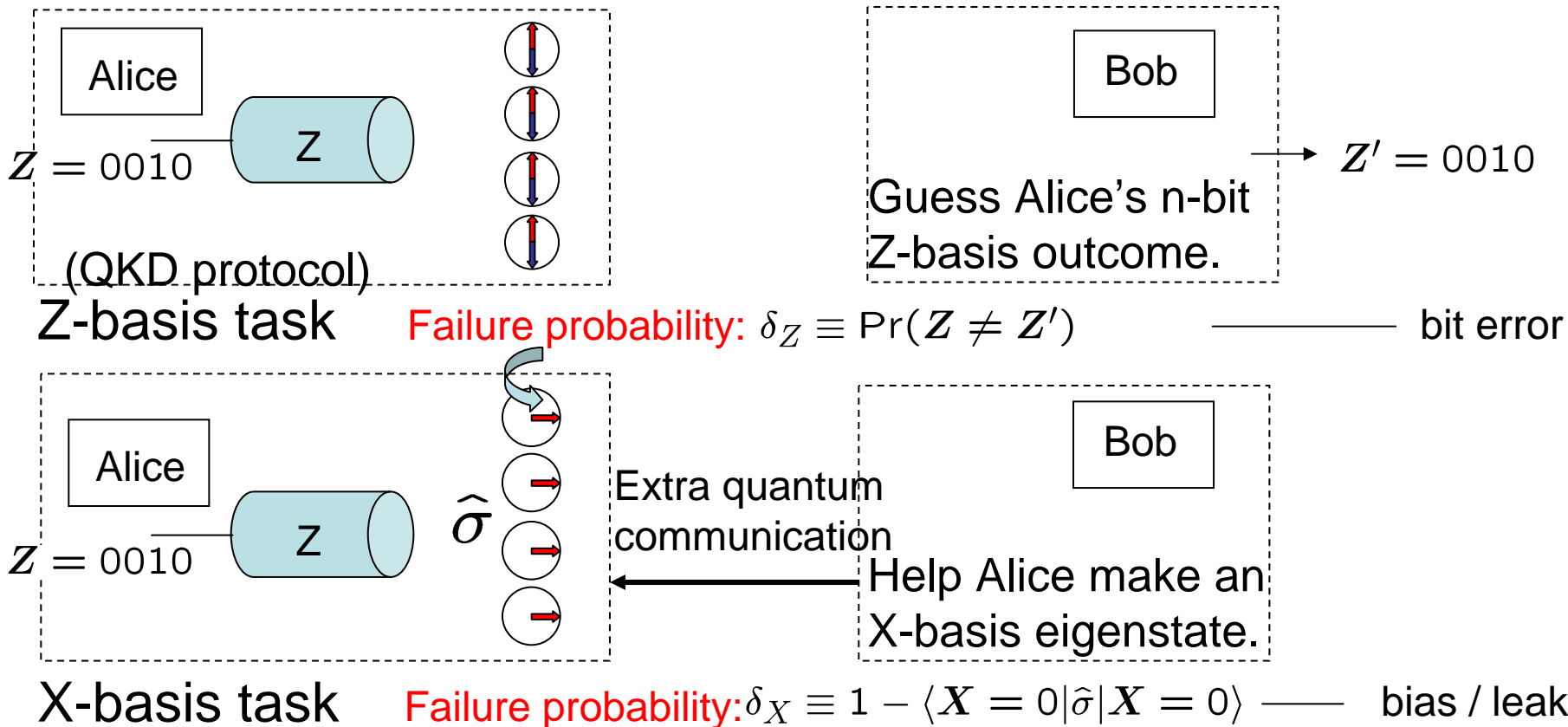
X-basis task



Perfectly random
No leak to Eve

Help Alice make an X-basis eigenstate.
(without disturbing the Z-basis observable)

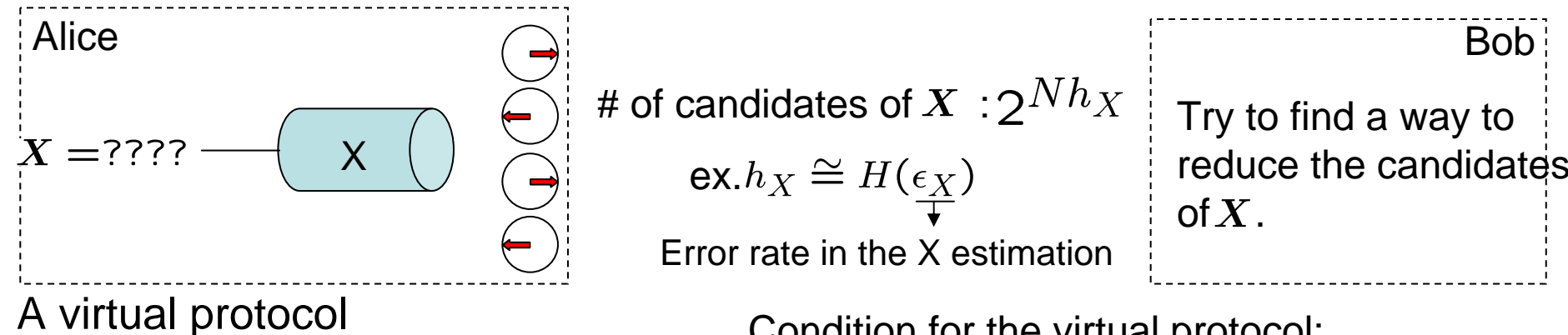
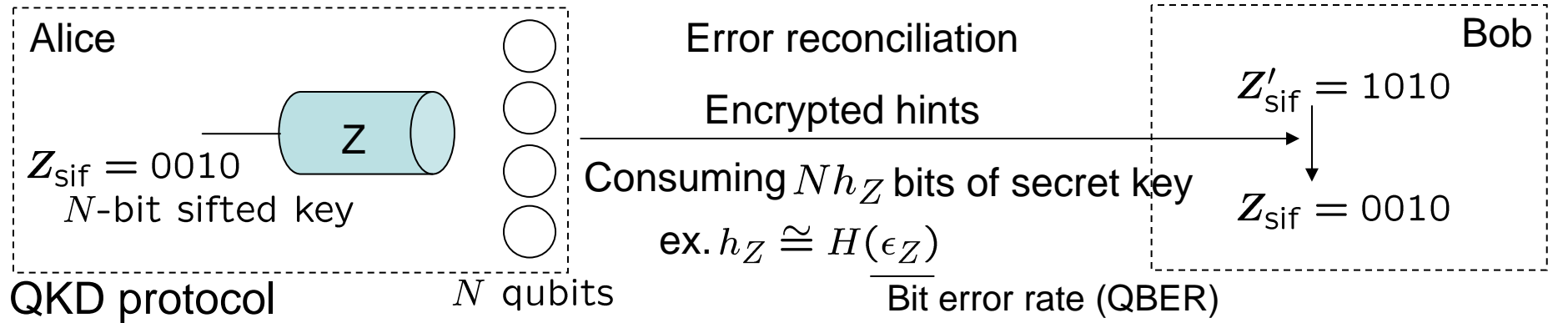
Effect of small imperfections



$$\left. \begin{aligned} \text{Final key: } \hat{\rho}_{ABE} &= \sum_{Z, Z'} p_{Z, Z'} |Z, Z'\rangle \langle Z, Z'|_{AB} \otimes \hat{\rho}_E^{(Z, Z')} \\ \text{Ideal key: } \hat{\tau}_{ABE} &= \sum_Z 2^{-n} |Z, Z\rangle \langle Z, Z|_{AB} \otimes \hat{\rho}_E \end{aligned} \right\} 1 - F(\hat{\tau}_{AE}, \hat{\rho}_{AE}) \leq \delta_X$$

$$\delta_{\text{key}} \equiv \|\hat{\tau}_{ABE} - \hat{\rho}_{ABE}\|_1 \leq 2\delta_Z + 2\sqrt{\delta_X}$$

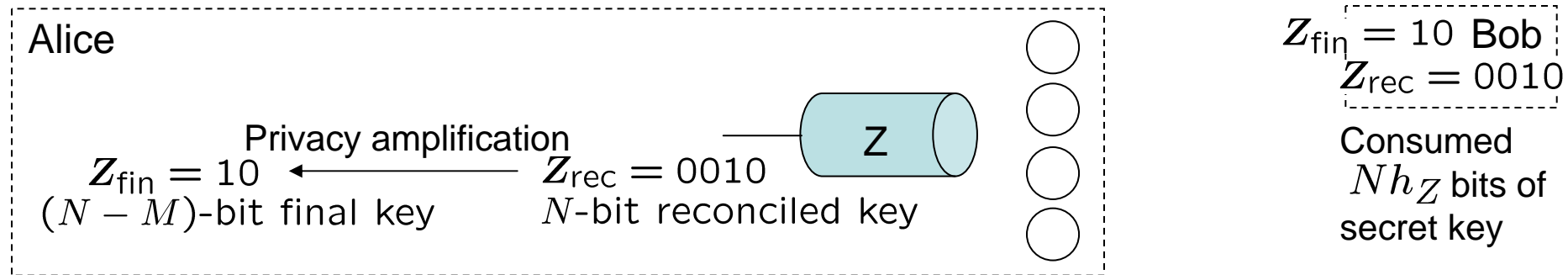
A prescription of deriving a lower bound on the key rate



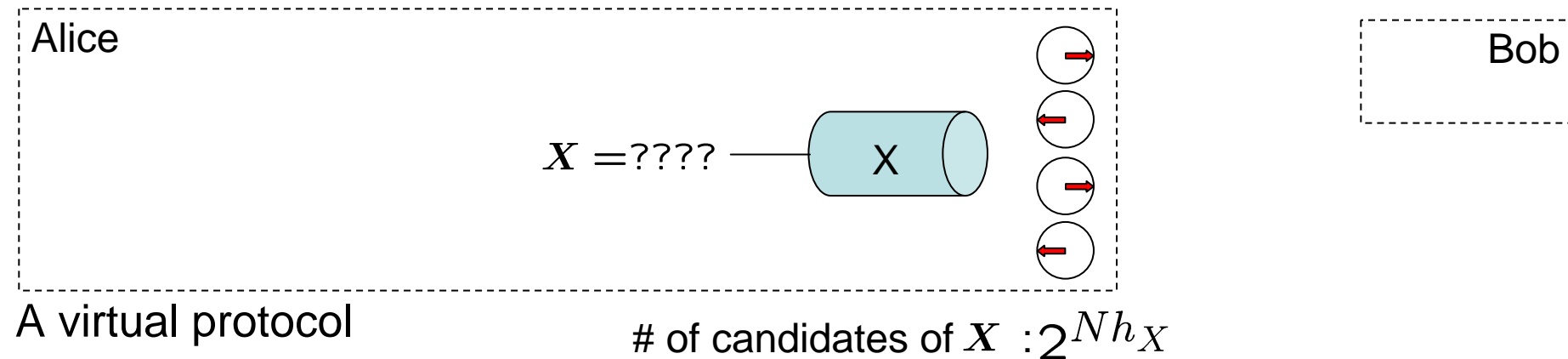
Condition for the virtual protocol:

- Do not disturb the Z value of the N qubits.
- Quantum channels can be freely used.

A prescription of deriving a lower bound on the key rate

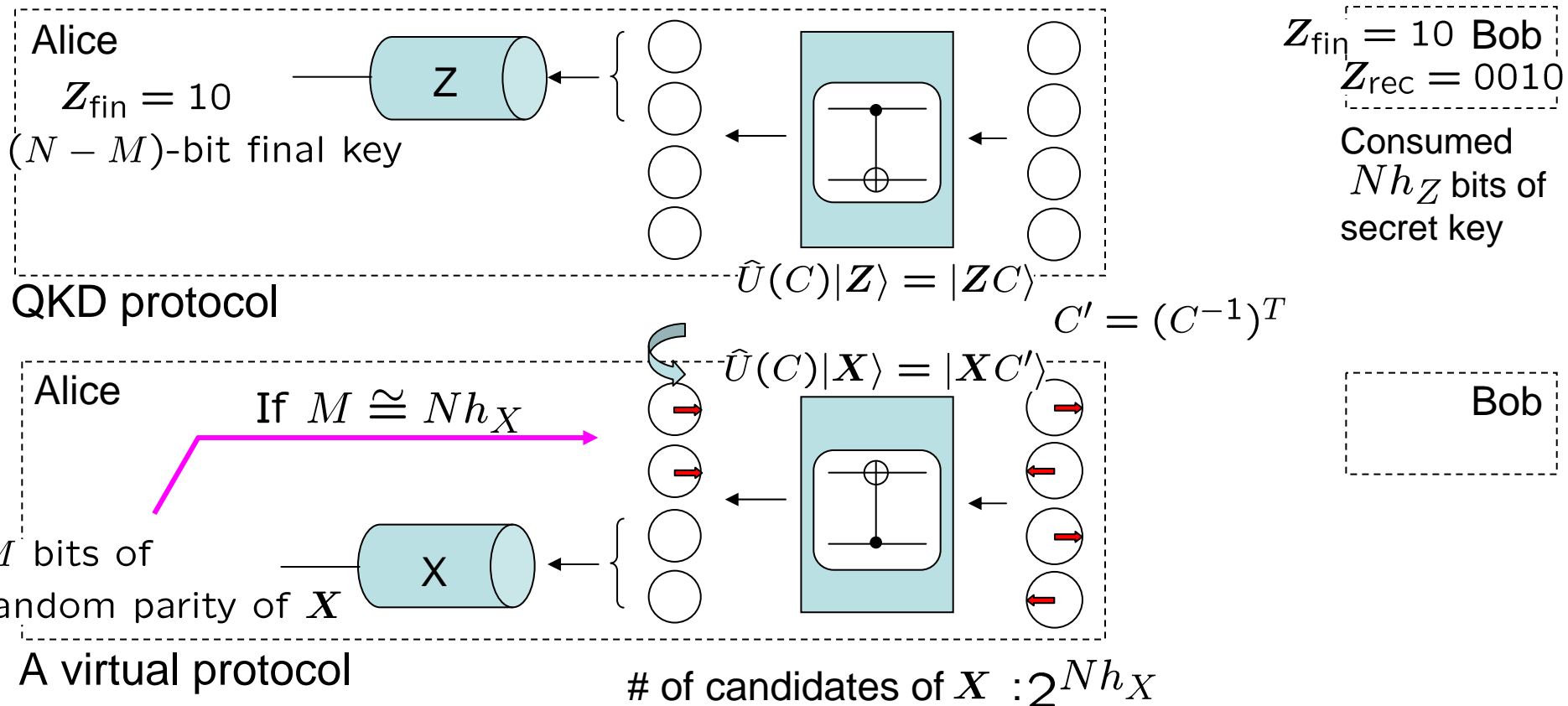


QKD protocol



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

A prescription of deriving a lower bound on the key rate



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

The final key is secure

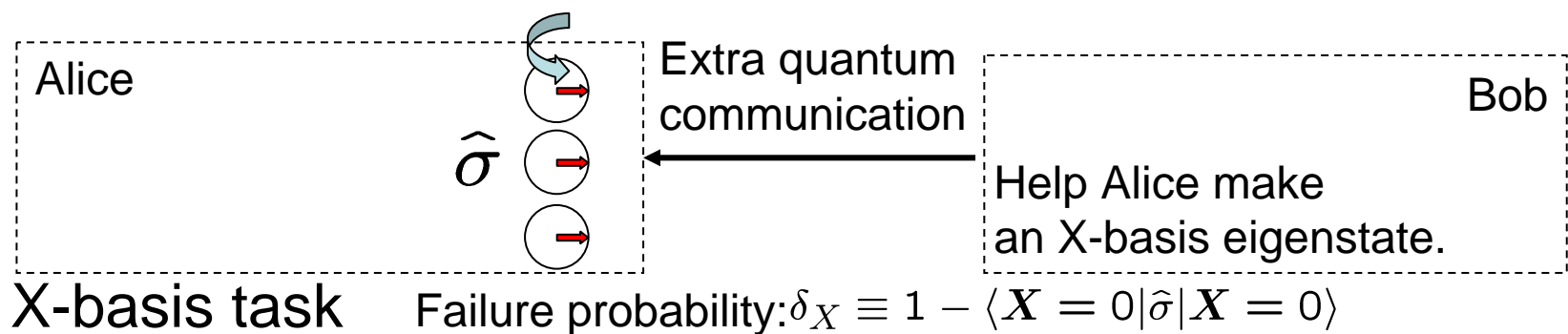
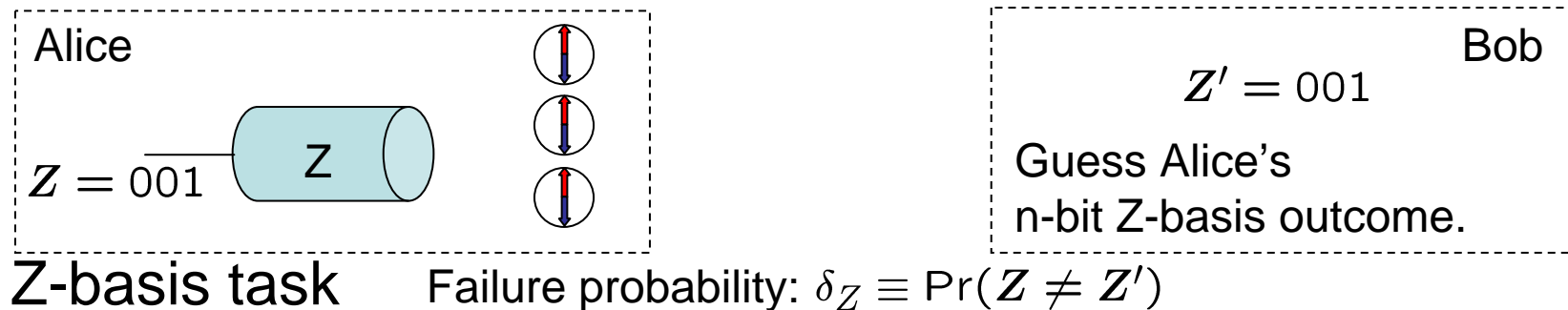
$$\text{Net key gain} = N(1 - h_X - h_Z)$$

Complementarity and security of quantum key distribution

Osaka Univ. Masato Koashi

- Proving the security of QKD via complementarity
 - Basic idea
 - Small imperfections
 - A prescription for determining the key rate
- Merits in the complementarity approach
 - Applicability and relation to entanglement
 - Security from an operationally defined quantity
- Examples (BB84, BBM92, 6-state protocols)
- Summary

QKD and complementarity



Secret key can be extracted with imperfection

$$\delta_{\text{key}} \equiv \|\hat{\tau}_{ABE} - \hat{\rho}_{ABE}\|_1 \leq 2\delta_Z + 2\sqrt{\delta_X}$$

The opposite is also true.

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

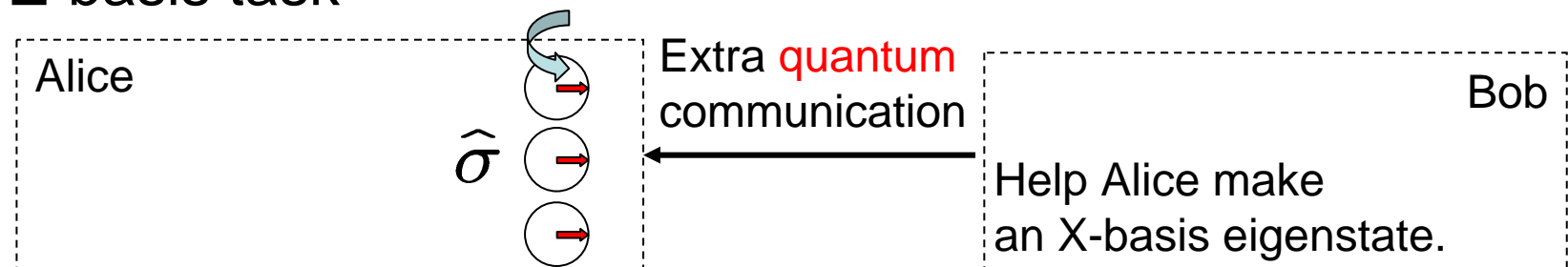
$$\delta_Z \leq \delta_{\text{key}}/2 \text{ and } \delta_X \leq \delta_{\text{key}} - (\delta_{\text{key}}/2)^2.$$

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

Operational measures of quantum correlations



Z-basis task



X-basis task

Define optimal yield $Y_Q(\rho_{AB})$ such that

$\rho_{AB}^{\otimes n} \xrightarrow{\text{LOCC}}$ the two tasks are feasible for $\sim nY_Q(\rho_{AB})$ qubits

Complementarity

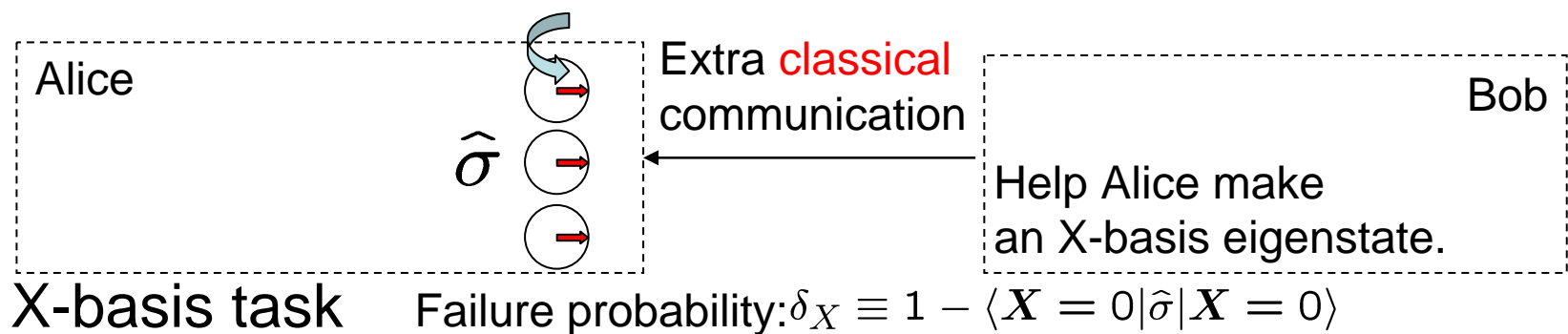
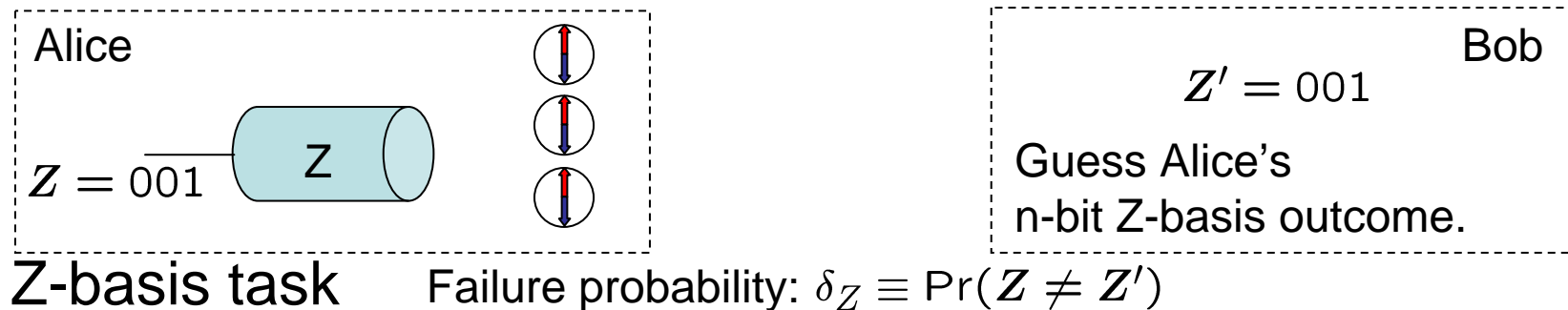
$$K_D(\rho_{AB}) = Y_Q(\rho_{AB})$$

Monogamy (exclusive correlations)

Distillable key: optimal yield $K_D(\rho_{AB})$ such that

$\rho_{AB}^{\otimes n} \xrightarrow{\text{Public comm.}} \sim nK_D(\rho_{AB})$ bits of secret key

Entanglement distillation and complementarity



➡ **EPR pairs** can be extracted with imperfection

$$\delta_{\text{ent}} \equiv \|\rho_{AB} - |\phi^{\text{mes}}\rangle\langle\phi^{\text{mes}}|_{AB}\|_1 \leq 4\sqrt{\delta_Z(1 - \delta_Z)} + 2\sqrt{\delta_X}$$

The opposite is trivial:

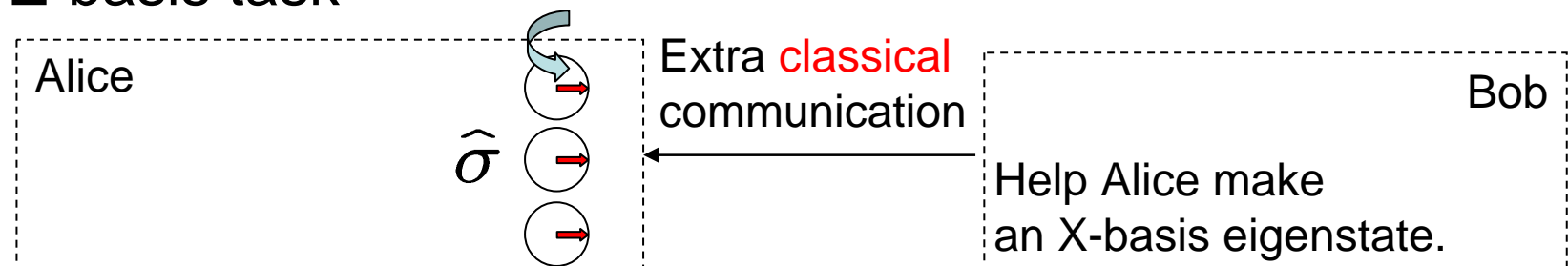
Whenever EPR pairs can be extracted with imperfection δ_{ent} ,
the two tasks are feasible with imperfections as small as

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

Operational measures of quantum correlations



Z-basis task



X-basis task

Define optimal yield $Y_C(\rho_{AB})$ such that

$\rho_{AB}^{\otimes n} \xrightarrow{\text{LOCC}}$ the two tasks are feasible for $\sim nY_C(\rho_{AB})$ qubits

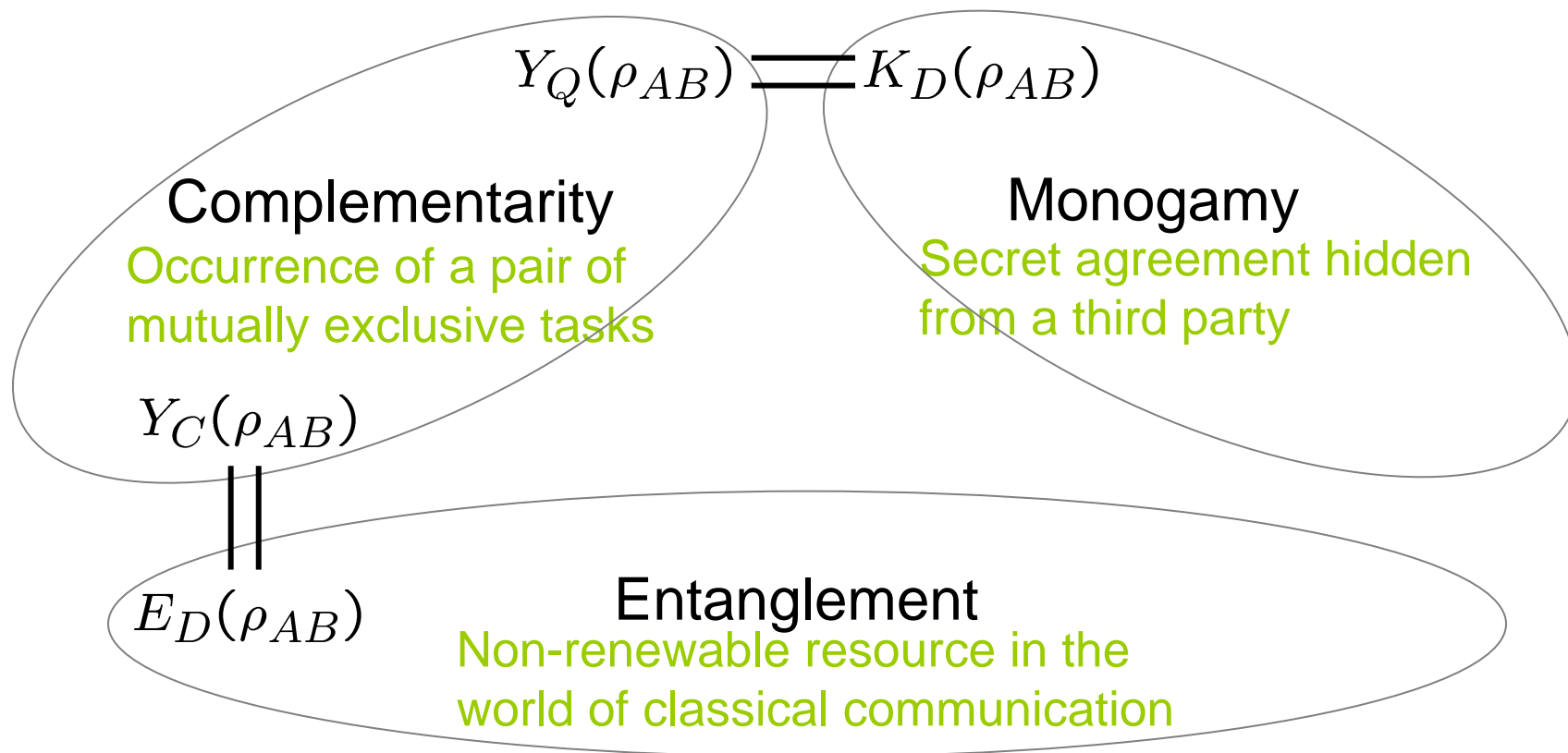
Complementarity

$$E_D(\rho_{AB}) = Y_C(\rho_{AB})$$

Entanglement (in reference to 'ebits')

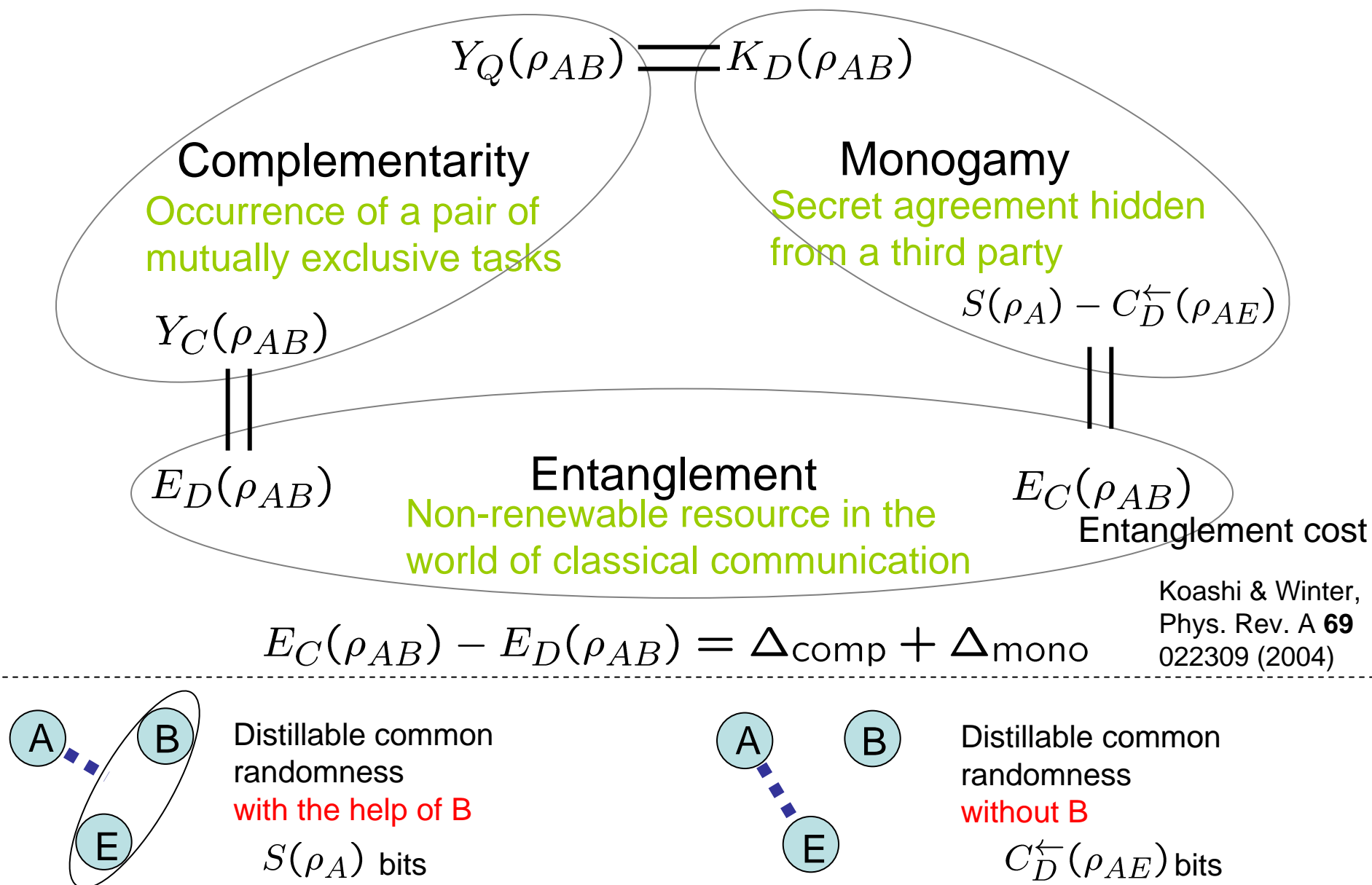
Distillable entanglement: optimal yield $E_D(\rho_{AB})$ such that

$\rho_{AB}^{\otimes n} \xrightarrow{\text{LOCC}} \sim nE_D(\rho_{AB})$ EPR pairs of qubits

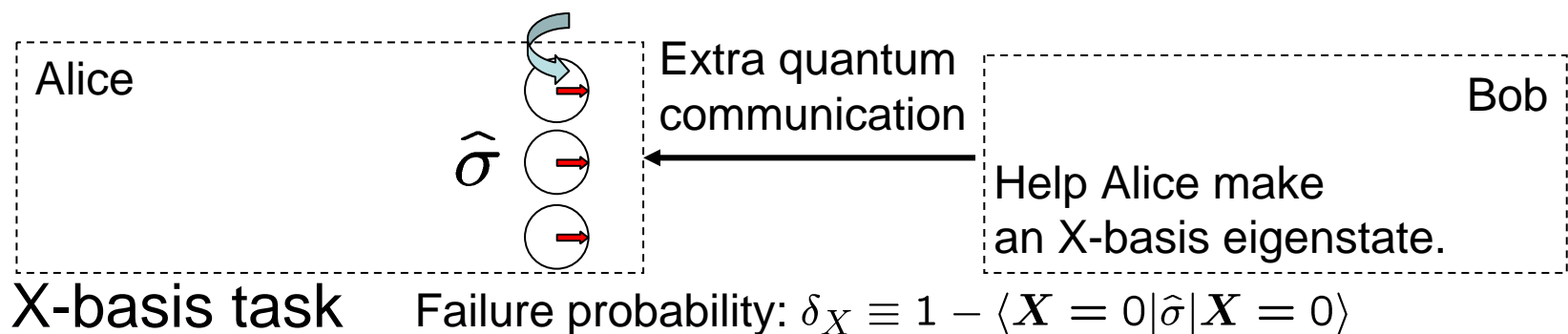
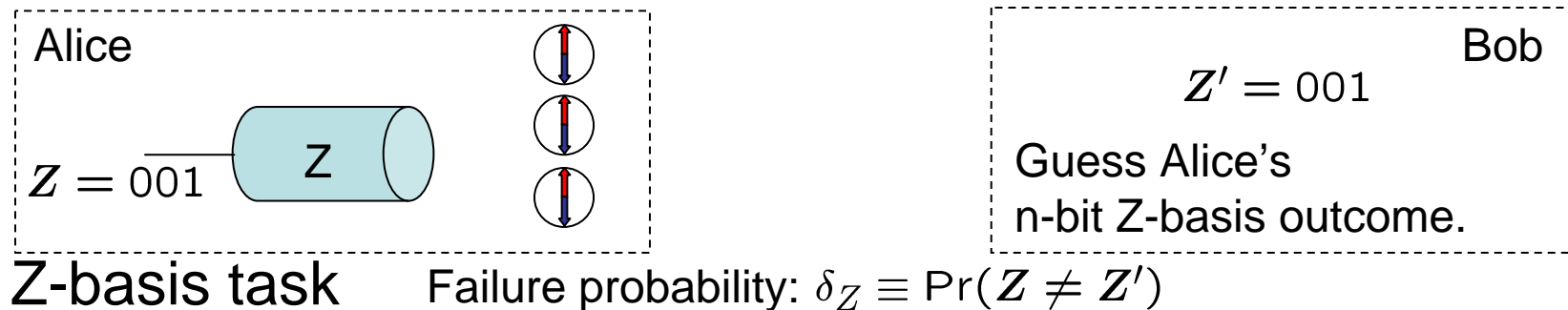



$$K_D(\rho_{AB})_{\text{(bits)}} - E_D(\rho_{AB})_{\text{(ebits)}} = \Delta_{\text{comp}} \equiv Y_Q(\rho_{AB}) - Y_C(\rho_{AB})$$

Operational measures of quantum correlations



Security from an operationally defined quantity



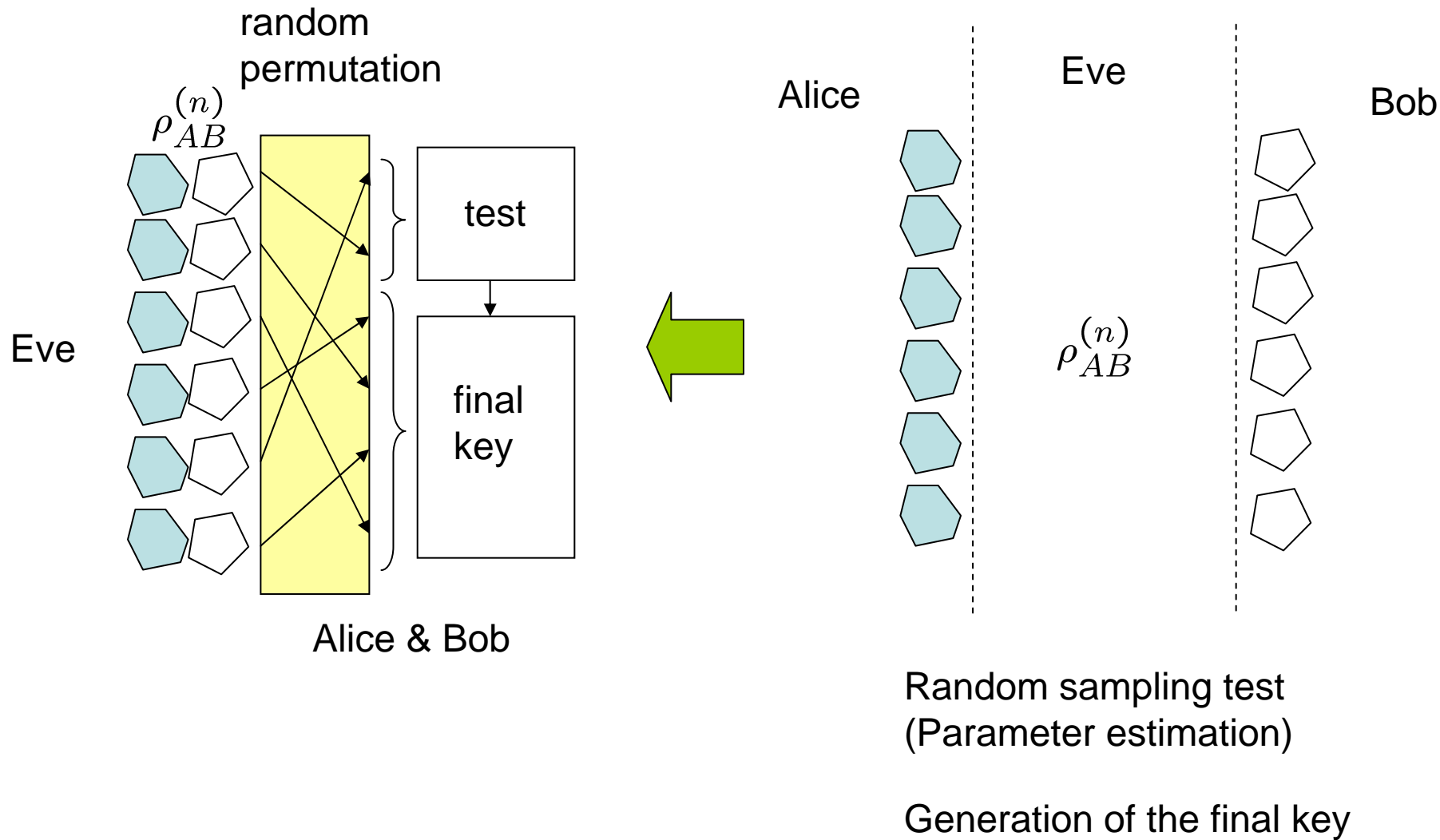

 $\delta_{\text{key}} \equiv \|\hat{\tau}_{ABE} - \hat{\rho}_{ABE}\|_1 \leq 2\delta_Z + 2\sqrt{\delta_X}$

The final security statement is obtained directly from an **operationally defined quantity**.

“Failure probability of a protocol.”

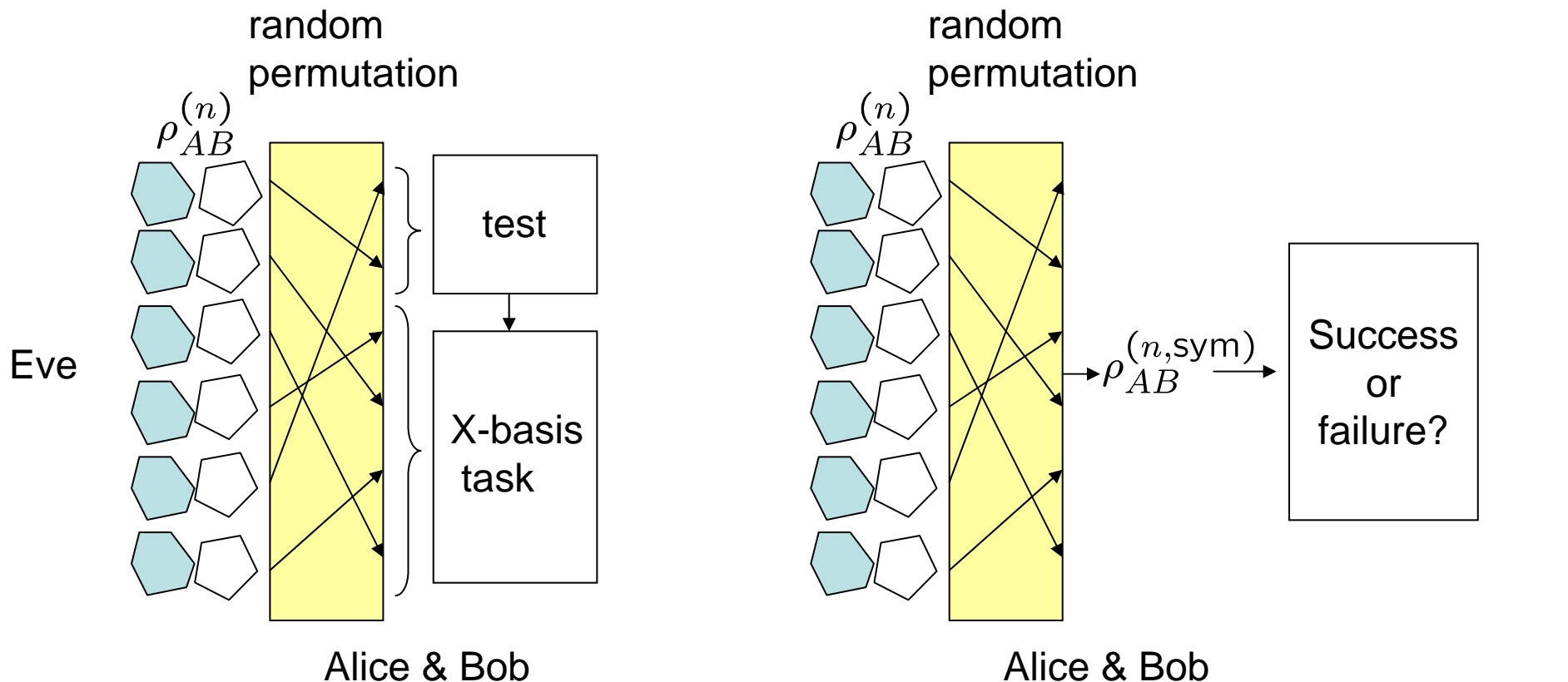
- The coherent attacks can be treated rather easily.
- Sometimes the security is established without knowing much about what is actually going on.

Treatment of coherent attacks



Treatment of coherent attacks

Tamaki, Koashi, Imoto, Phys. Rev. Lett. **90**, 167904 (2003).



How large is the failure probability δ_X ?

$$\delta_X = p(\rho_{AB}^{(n, \text{sym})}) \equiv \text{tr}(\hat{F}_{\text{fail}} \rho_{AB}^{(n, \text{sym})})$$

Security analysis for individual attacks (“relatively easy”)

$$p(\rho_{AB}^{\otimes n}) \sim o(e^{-cn}) \quad \forall \rho_{AB}$$

Assume that this is confirmed. What can we say about $p(\rho_{AB}^{(n, \text{sym})})$?

Treatment of coherent attacks

Tamaki, Koashi, Imoto, Phys. Rev. Lett. **90**, 167904 (2003).

$$\delta_X = p(\rho_{AB}^{(n,\text{sym})}) \equiv \text{tr}(\hat{F}_{\text{fail}} \rho_{AB}^{(n,\text{sym})})$$

Assume that the following has been proved for individual attacks.

$$p(\rho_{AB}^{\otimes n}) \sim o(e^{-cn}) \quad \forall \rho_{AB}$$

As long as the dimension is finite,

$$\mathcal{H}_{AB}^{\otimes n} = \bigoplus_Y \mathcal{R}_Y \otimes \mathcal{S}_Y$$

Y : Young diagrams [# is poly(n)]
 \mathcal{R}_Y : irrep. of $SU(d)$ [dim. is poly(n)]
 \mathcal{S}_Y : irrep. of S_n

$\hat{U} \otimes \hat{U} \otimes \hat{U} \otimes \dots \otimes \hat{U}$ Permutation of systems

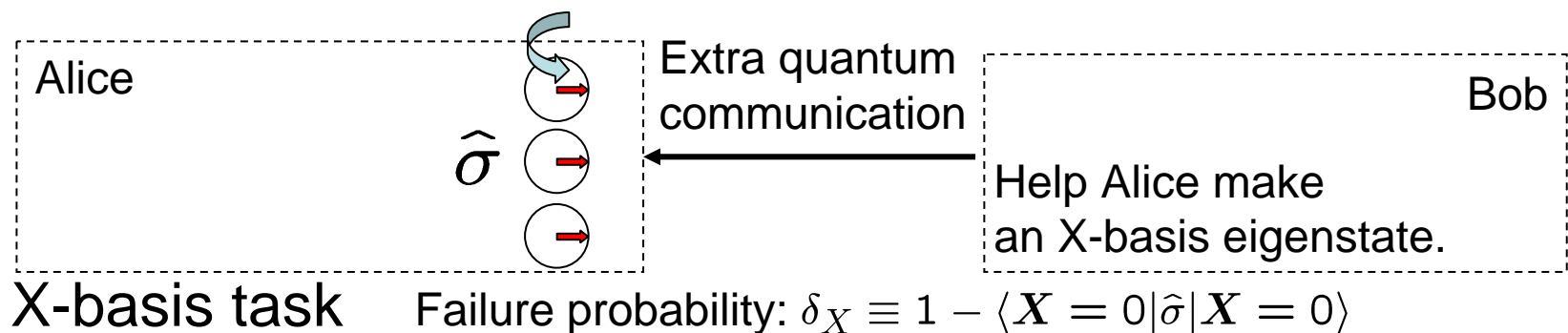
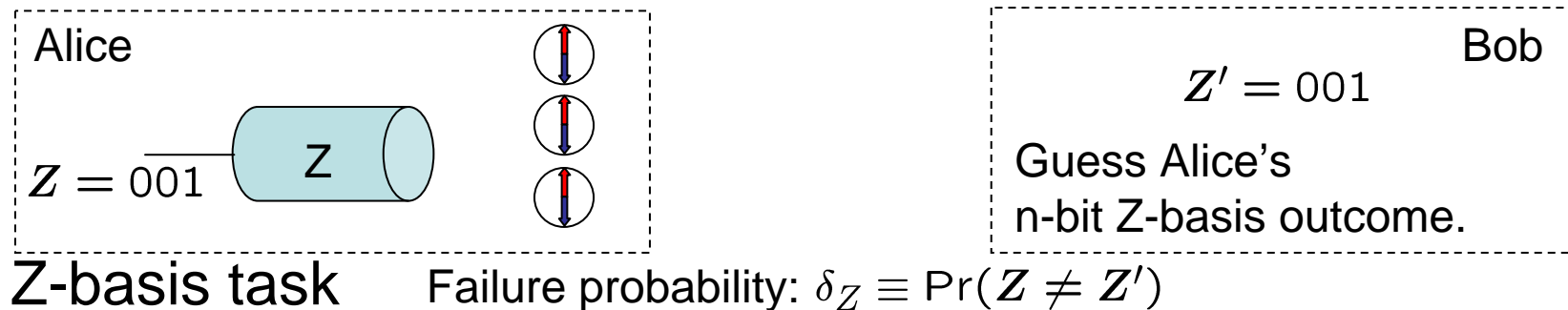
$$\rho_{AB}^{(n,\text{sym})} = \bigoplus_Y p_Y \sigma_Y \otimes \frac{\hat{1}_Y}{\dim \mathcal{S}_Y}$$


All Eve can do is
tweak the “poly” parts.

$\exists Y, \rho_{AB}$

$$\begin{aligned}
 p(\rho_{AB}^{(n,\text{sym})}) &\leq p\left(\sigma_Y \otimes \frac{\hat{1}_Y}{\dim \mathcal{S}_Y}\right) \leq \dim \mathcal{R}_Y p\left(\frac{\hat{1}_Y}{\dim \mathcal{R}_Y} \otimes \frac{\hat{1}_Y}{\dim \mathcal{S}_Y}\right) \\
 &\leq \text{poly}(n) p(\rho_{AB}^{\otimes n}) \sim o(e^{-cn})
 \end{aligned}$$

Security from an operationally defined quantity



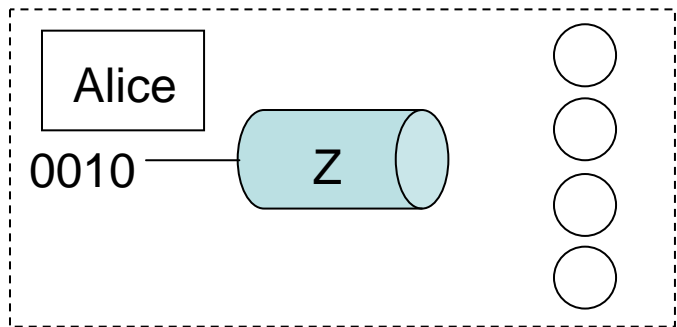

 $\delta_{\text{key}} \equiv \|\hat{\tau}_{ABE} - \hat{\rho}_{ABE}\|_1 \leq 2\delta_Z + 2\sqrt{\delta_X}$

The final security statement is obtained directly from an **operationally defined quantity**.

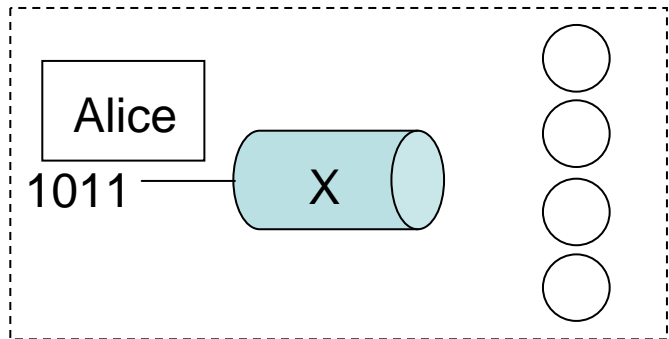
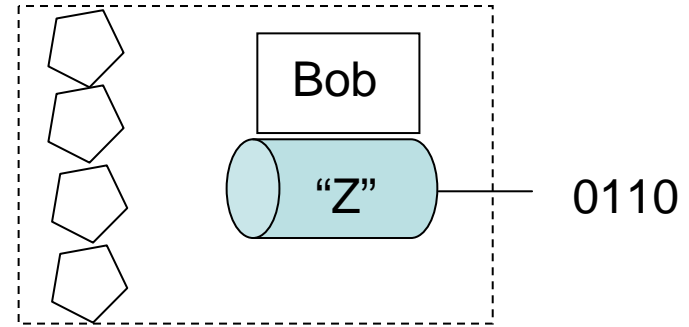
“Failure probability of a protocol.”

- The coherent attacks can be treated rather easily.
- Sometimes the security is established without knowing much about what is actually going on.

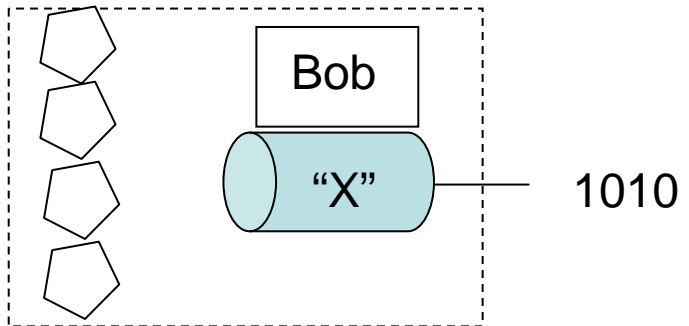
BB84 protocol (BBM92 protocol)



(REAL)
Z basis chosen
Error rate: ϵ_Z



(REAL)
X basis chosen
Error rate: ϵ_X



Assumption:

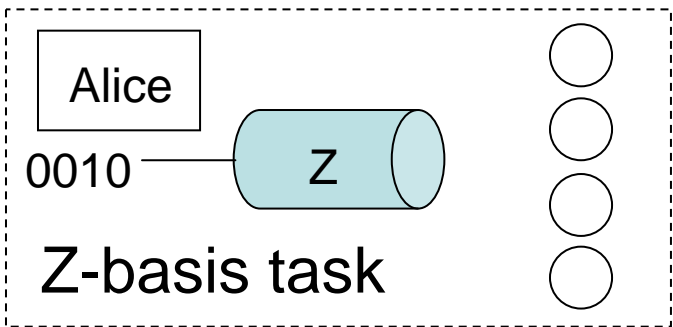
Alice's measurement is ideal.

- Ideal single-photon signal states in BB84.
- Ideal measurements on a single photon in BBM92.

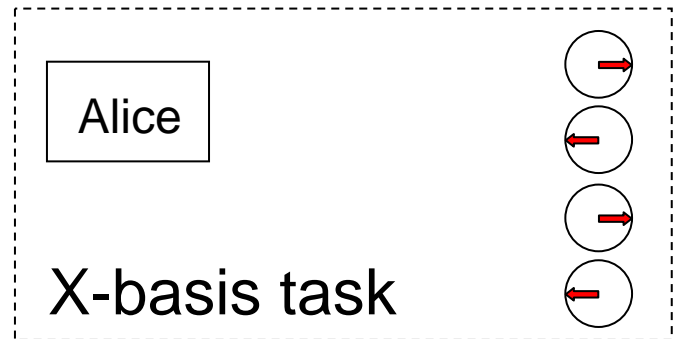
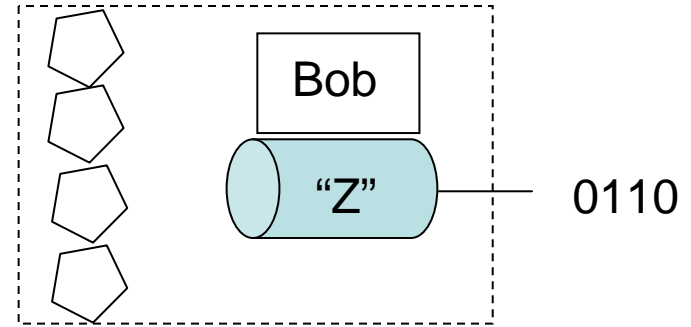
Assumption:

Bob's measurement can be anything as long as the detection efficiency is basis independent.

BB84 protocol (BBM92 protocol)



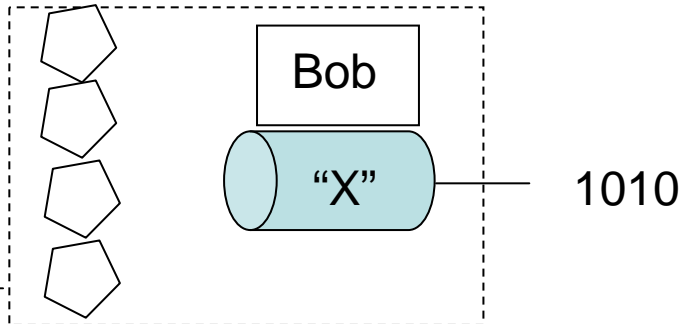
(REAL)
Z basis chosen



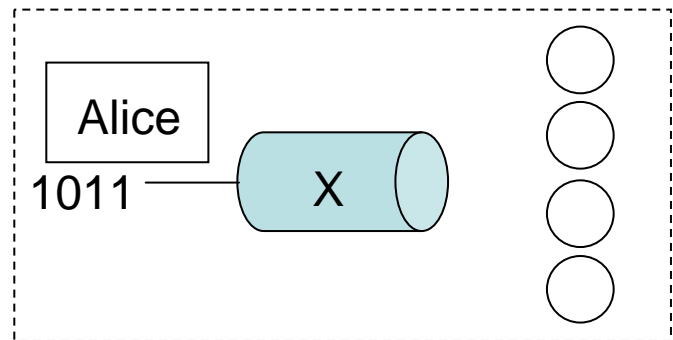
(VIRTUAL)

Error rate: $\tilde{\epsilon}_X$

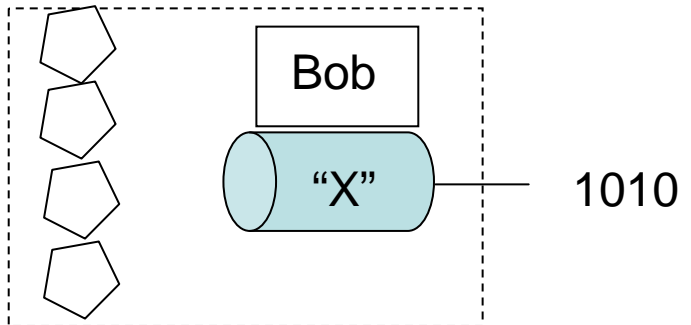
Extra classical
communication



$2^{NH(\tilde{\epsilon}_X)}$ candidates of X value



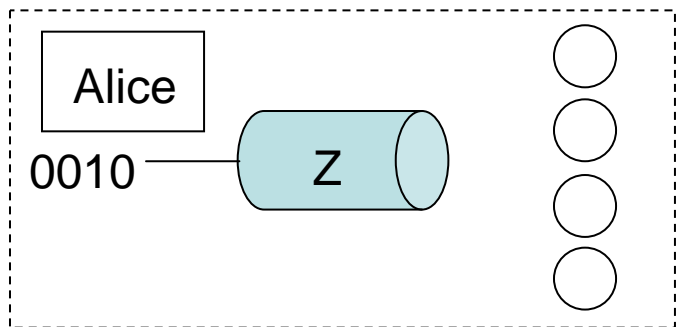
(REAL)
X basis chosen
Error rate: ϵ_X



The detection efficiency is basis independent.

→ The real protocol is a fair sampling of the virtual one. $\tilde{\epsilon}_X = \epsilon_X$

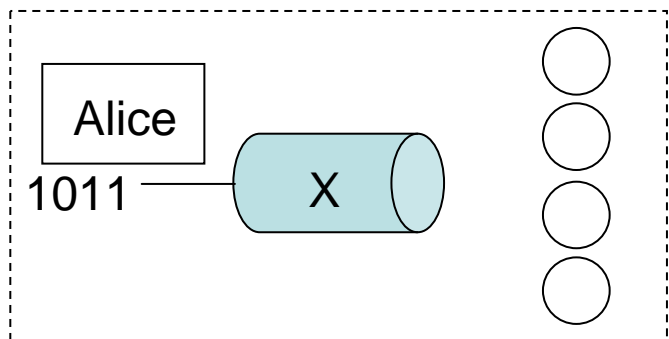
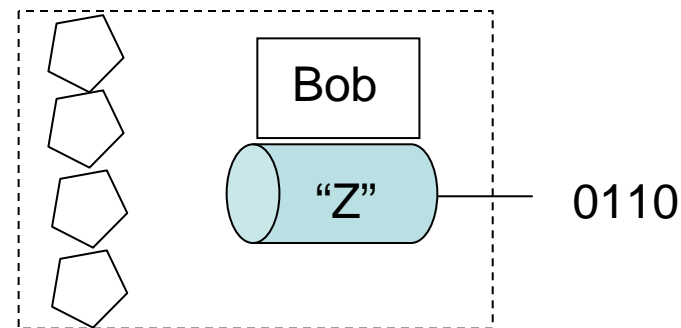
BB84 protocol (BBM92 protocol)



(REAL)

Z basis chosen

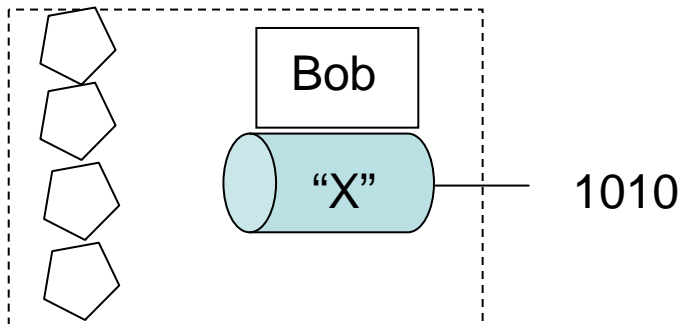
Error rate: ϵ_Z



(REAL)

X basis chosen

Error rate: ϵ_X



Assumption:

Alice's measurement is ideal.

- Ideal single-photon signal states in BB84.
- Ideal measurements on a single photon in BBM92.

Assumption:

Bob's measurement can be anything as long as the detection efficiency is basis independent.

Key gain

$$N[1 - H(\epsilon_Z) - H(\epsilon_X)]$$

basis-dependence \longrightarrow

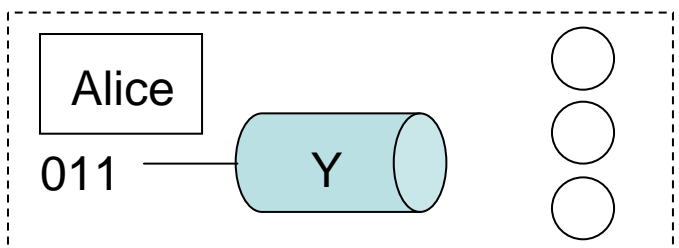
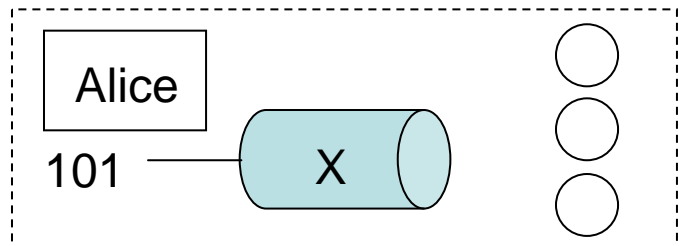
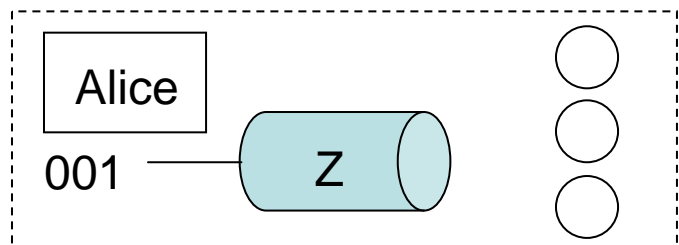
Fung, Tamaki, Qi, Lo, Ma (2008)

Lydersen, Skaar (2008)

Relaxing the detection models **does not** change the key rate.

6-state protocol

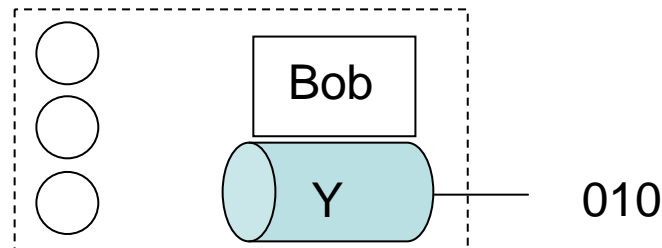
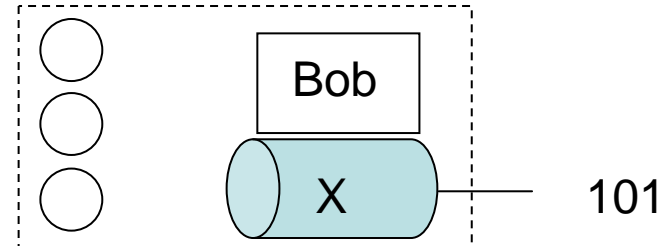
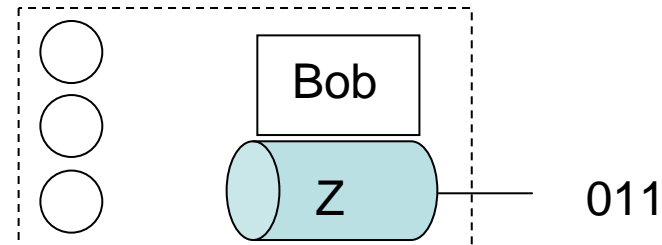
Lo (2001)



(REAL)
Z basis chosen
Error rate: ϵ_Z

(REAL)
X basis chosen
Error rate: ϵ_X

(REAL)
Y basis chosen
Error rate: ϵ_Y



$$\text{BB84: } N[1 - H(\epsilon_Z) - H(\epsilon_X)]$$

$$\text{6-state } N[1 - H(\epsilon_Z) - h_X]$$

$$h_X = \text{"H(X|Z)"}$$

$$= (1 - \epsilon_Z)H(\epsilon_0) + \epsilon_Z H(\epsilon_1)$$

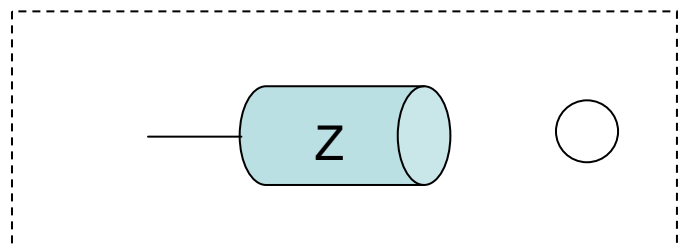
$$\epsilon_X = (1 - \epsilon_Z)\epsilon_0 + \epsilon_Z \epsilon_1$$

$$h_X \sim H(\epsilon/2)$$

	Z error		
X error	1	$\epsilon/2$	ϵ_X
	$\epsilon/2$	$\epsilon/2$	
	ϵ_Y	ϵ_Z	

For $\epsilon_X = \epsilon_Y = \epsilon_Z = \epsilon \ll 1$

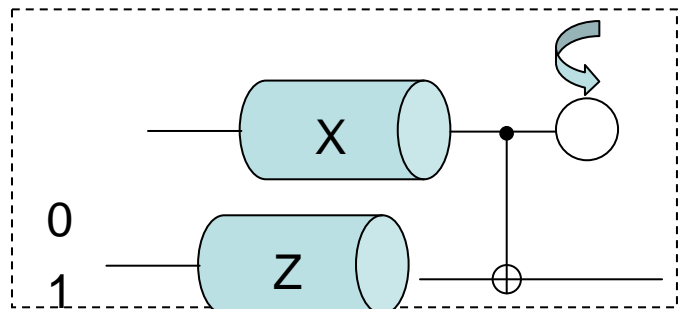
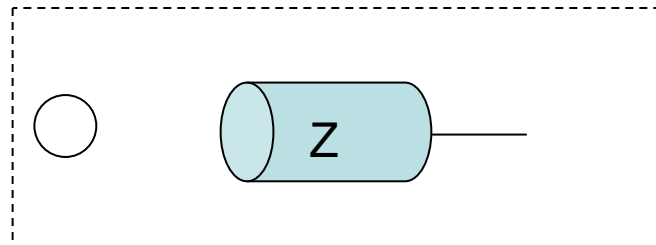
6-state protocol



(REAL)

Z basis chosen

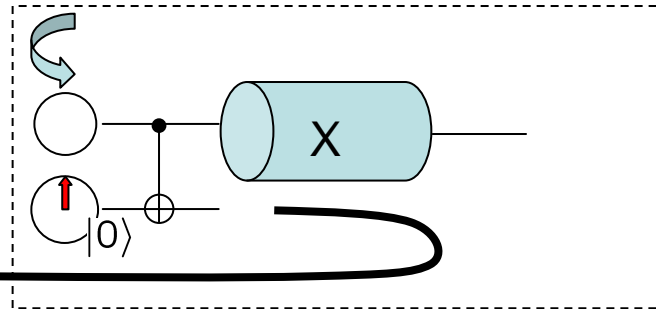
Error rate: ϵ_Z



(VIRTUAL)

Error rate: ? ϵ_0 ϵ_1

Extra **quantum**
communication

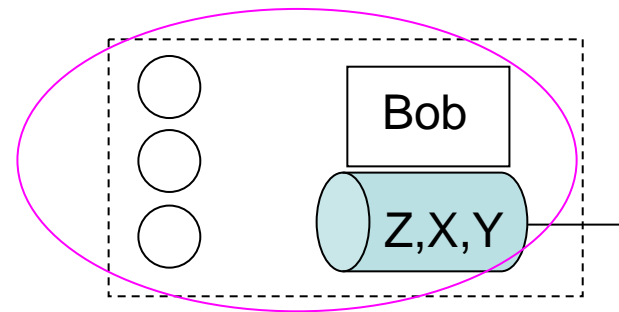
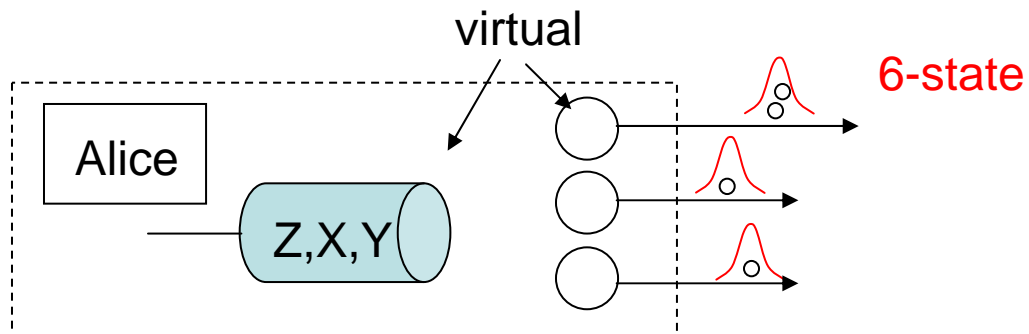
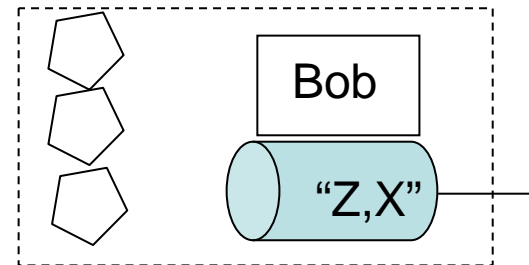
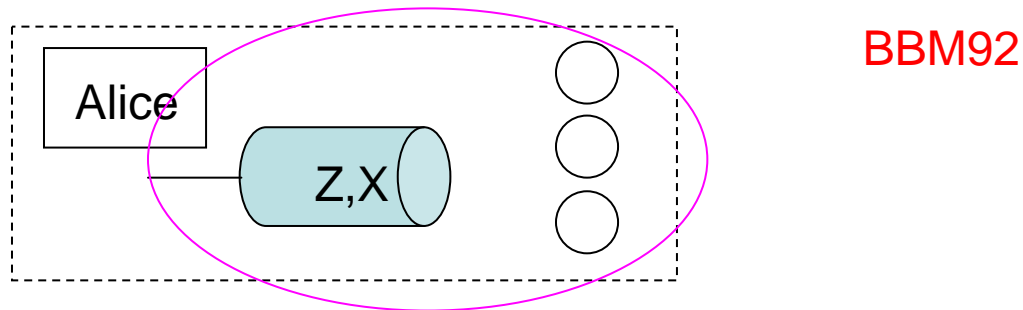
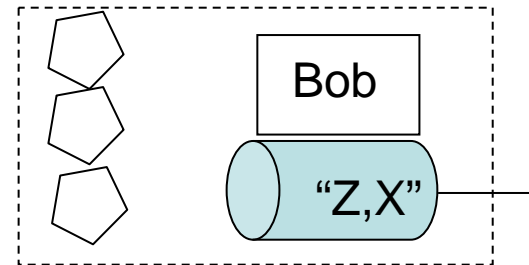
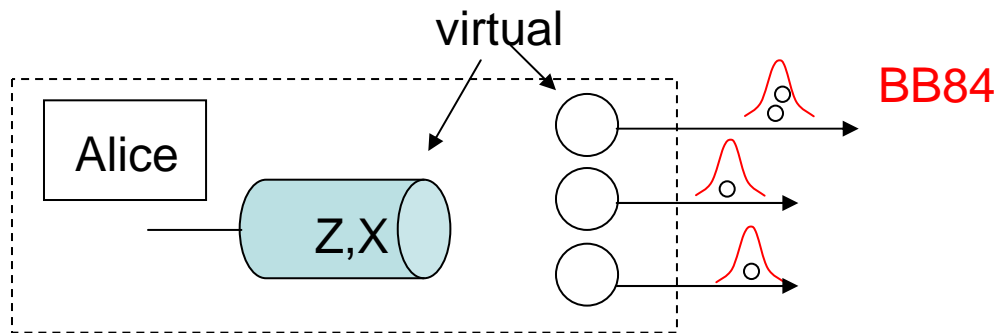


In the complementarity argument, how we may define something like $H(X|Z)$?

$$h_X = (1 - \epsilon_Z)H(\epsilon_0) + \epsilon_Z H(\epsilon_1)$$

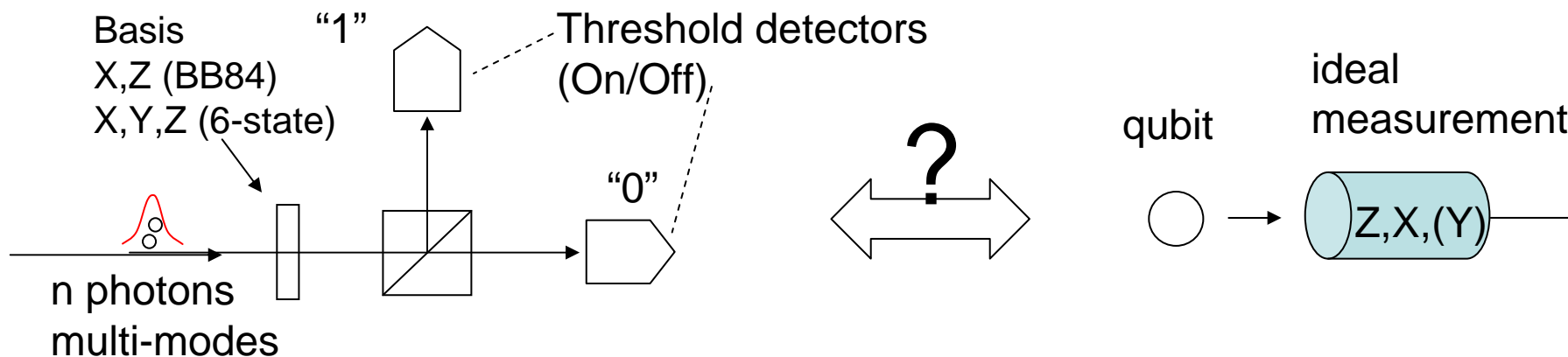
$$\epsilon_X = (1 - \epsilon_Z)\epsilon_0 + \epsilon_Z \epsilon_1$$

How to assign a qubit in various protocols



We have to interpret the actual measurement as an ideal measurement on a qubit. (Problem in Quantum Optics)

How to assign a qubit in the actual measurement?



Squashing approach

Protocol independent

Single counting \longrightarrow 0, 1
 Double counting $\xrightarrow{\text{(Random guess)}}$ 0, 1

An increased error fraction,
 but no “multi-photon” event

$$R_{\text{key}} = 1 - 2H\left(\epsilon + \frac{\delta}{2}\right)$$

$1 - \epsilon - \delta$: no error

ϵ : bit error

δ : double counting

Tsurumaru and Tamaki, arXiv:0803.4226

Beaudry, Moroder, Lutkenhaus, arXiv:0804.3082

Separating approach

Not depending on “luck”

Ex. 6-state protocol

Single counting \longrightarrow 0, 1
 Double counting \longrightarrow Publicly announce as it is.

The error fraction is unaltered,
 but “multi-photon” events occur.

$$R_{\text{key}} = (1 - 4\delta)\left[1 - H\left(\frac{\epsilon}{1 - 4\delta}\right)\right] - (1 - \delta)H\left(\frac{\epsilon}{1 - \delta}\right)$$

Koashi, Yamamoto, Adachi, Imoto, arXiv:0804.0891

Summary

The complementarity argument is a useful tool for the security proof of QKD.

The final security statement is obtained directly from operationally defined quantities, failure probabilities of a pair of protocols.

- The coherent attacks can be treated rather easily.
- Sometimes the security is established without knowing much about what is actually going on.

The feasibility of the pair of tasks is ‘equivalent’ to achievability of secret key.

- The complementarity approach is, in principle, applicable to any QKD scheme.
- Helps to clarify the relations among various operationally defined measures of quantum correlations.