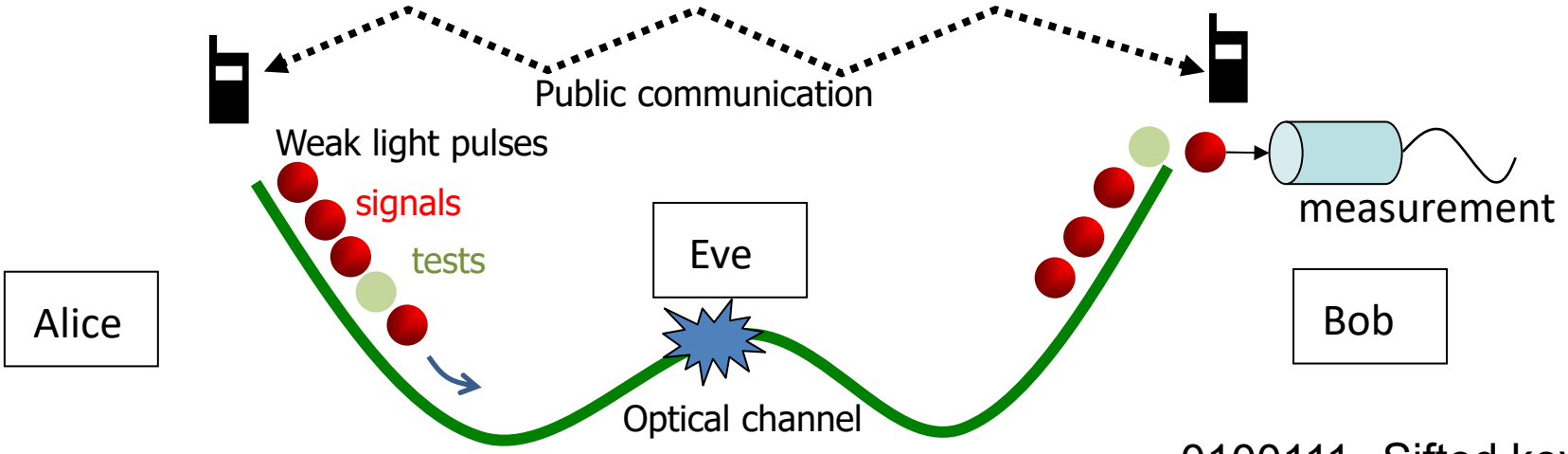
QCrypt2020: Aug. 12, 2020

Tutorial: Security of quantum key distribution: approach from complementarity

Univ. of Tokyo　Masato Koashi

Quantum key distribution (QKD)



Sifted key 0100101 0100111 Sifted key

Error correction

0100101 ??0?1?? 0100101

Estimating the amount of leak from observed test data

Privacy amplification

Final key 0101 ???? 0101 Final key

Shortening the key to remove the leaked portion

Aim of this tutorial

Explain how we can prove the security of QKD protocols against general attacks,

focusing on the approach with “phase errors,”
which dates back to Mayers, Shor and Preskill.

PART I: Methodology

Step 1: Perfect world (Basic idea)

Step 2: Almost perfect world (Composable security)

Step 3: Practical world (Privacy amplification)

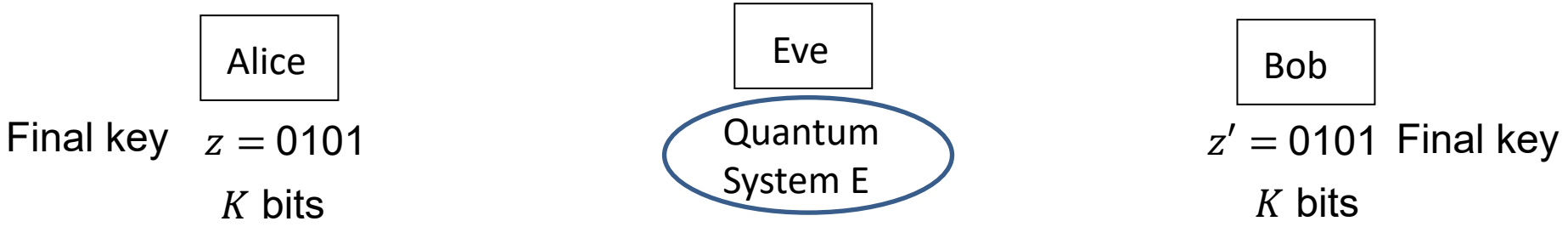
PART II: Protocols

BB84
B92
TF-QKD
RRDPS
DM-CV QKD

STEP 1: Perfect world

Goal of QKD

Ideal property of the final key



- Correlation-free $\rho_{\mathrm{E}}(z, z') = \rho_{\mathrm{E}} \ \forall z, z'$
- Uniformly distributed $\sum_{z'} p(z, z') = \sum_{z} p(z, z') = 2^{-K}$
- Error-free $p(z, z') = 0$ whenever $z \neq z'$

Quantum description

General state:
$$\rho_{\mathrm{ABE}}^{\mathrm{fin},K} = \sum_{z,z'=0}^{2^K-1} p(z, z') |z\rangle\langle z|_{\mathrm{A}} \otimes |z'\rangle\langle z'|_{\mathrm{B}} \otimes \rho_{\mathrm{E}}(z, z')$$

Ideal state:
$$\rho_{\mathrm{ABE}}^{\mathrm{ideal},K} = \sum_{z=0}^{2^K-1} 2^{-K} |z\rangle\langle z|_{\mathrm{A}} \otimes |z\rangle\langle z|_{\mathrm{B}} \otimes \rho_{\mathrm{E}}$$

Dividing the requirement

Ideal property of the final key

Alice

Eve

Bob

Final key $z = 0101$ K bits

Quantum System E

$z' = 0101$ Final key K bits

Overall security

- Correlation-free $\rho_{\mathrm{E}}(z, z') = \rho_{\mathrm{E}} \ \forall z, z'$
- Uniformly distributed $\sum_{z'} p(z, z') = \sum_{z} p(z, z') = 2^{-K}$
- Error-free $p(z, z') = 0$ whenever $z \neq z'$

Secrecy (for Alice)

$\rho_{\mathrm{E}}(z) = \rho_{\mathrm{E}} \ \forall z$ $\quad \mathrm{Prob}(z) = 2^{-K}$

Correctness

$\mathrm{Prob}(z, z') = 0$ whenever $z \neq z'$

Property of $\rho_{\mathrm{AE}}^{\mathrm{fin},K} := \mathrm{Tr}_{\mathrm{B}}(\rho_{\mathrm{ABE}}^{\mathrm{fin},K})$

General state: $\rho_{\mathrm{AE}}^{\mathrm{fin},K} = \sum_{z=0}^{2^K-1} p(z)|z\rangle\langle z|_{\mathrm{A}} \otimes \rho_{\mathrm{E}}(z)$

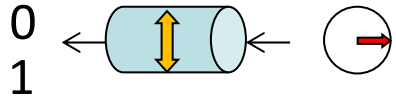
Ideal state: $\rho_{\mathrm{AE}}^{\mathrm{ideal},K} = \sum_{z=0}^{2^K-1} 2^{-K}|z\rangle\langle z|_{\mathrm{A}} \otimes \rho_{\mathrm{E}}$

Starting point: Cases when it is obviously secure

In what situation are we sure of achieving the ideal state?

$$\rho_{\mathrm{AE}}^{\mathrm{ideal},K} = \sum_{z=0}^{2^K-1} 2^{-K} |z\rangle\langle z|_{\mathrm{A}} \otimes \rho_{\mathrm{E}}$$

- Correlation-free
- Uniformly distributed



$$|+\rangle = (|0\rangle + |1\rangle)/\sqrt{2}$$

Z basis measurement

X basis eigenstate (a pure state)

H/V polarization

Output ports of a half beam splitter

Z component of spin

Circularly polarized photon

A single photon fed to one input port

1/2-Spin particle pointing (+x) direction

If system A is in a pure state, it has no correlation to another system.

contrapositive

If system A has non-zero correlation to another system, it is in a mixed state.

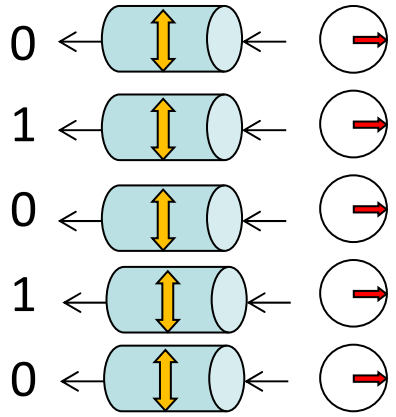
Starting point: Cases when it is obviously secure

In what situation are we sure of achieving the ideal state?

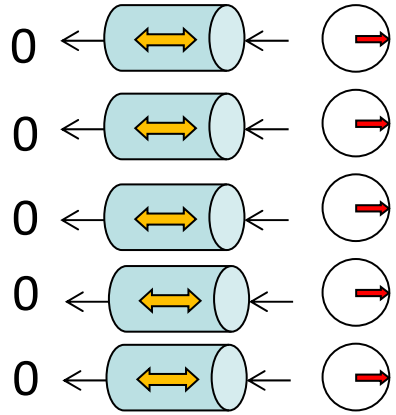
$$\rho_{\mathrm{AE}}^{\mathrm{ideal},K} = \sum_{z=0}^{2^K-1} 2^{-K} |z\rangle\langle z|_{\mathrm{A}} \otimes \rho_{\mathrm{E}}$$

- Correlation-free
- Uniformly distributed

$\rho_{\mathrm{AE}}^{\mathrm{ideal},K}$



$$|+\rangle = (|0\rangle + |1\rangle)/\sqrt{2}$$



Let us define the outcome '0000000' as 'success'.
Any other outcome is a failure.

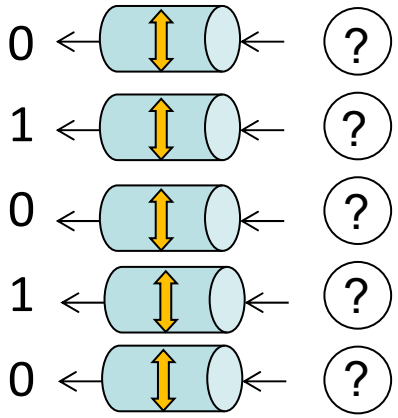
Starting point: Cases when it is obviously secure

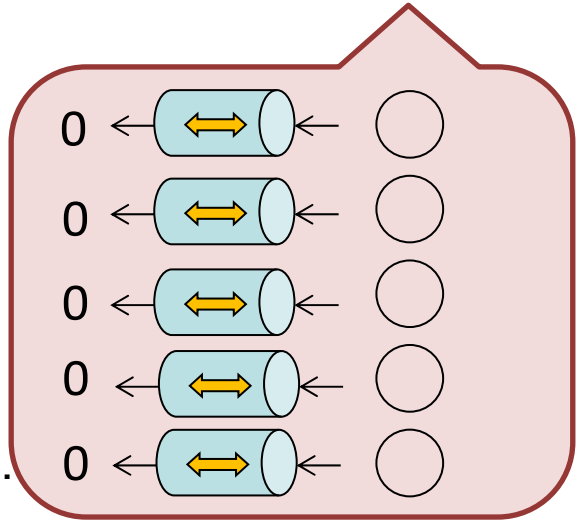
In what situation are we sure of achieving the ideal state?

$$\rho_{\mathrm{AE}}^{\mathrm{ideal},K} = \sum_{z=0}^{2^K-1} 2^{-K} |z\rangle\langle z|_{\mathrm{A}} \otimes \rho_{\mathrm{E}}$$

- Correlation-free
- Uniformly distributed

$\rho_{\mathrm{AE}}^{\mathrm{fin},K}$





If there is a promise that the failure probability is zero,

$$\rho_{\mathrm{AE}}^{\mathrm{fin},K} = \rho_{\mathrm{AE}}^{\mathrm{ideal},K}$$

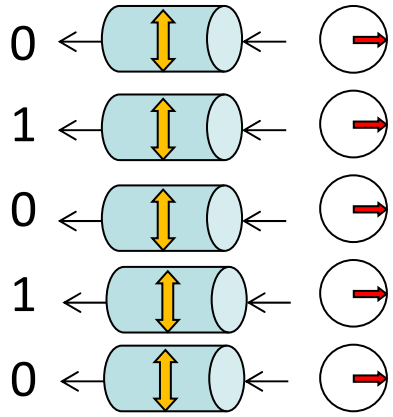
Let us define the outcome '0000000' as 'success'.
Any other outcome is a failure.

So what?

In what situation are we sure of achieving the ideal state?

$$\rho_{\mathrm{AE}}^{\mathrm{ideal},K} = \sum_{z=0}^{2^K-1} 2^{-K} |z\rangle\langle z|_{\mathrm{A}} \otimes \rho_{\mathrm{E}}$$

$\rho_{\mathrm{AE}}^{\mathrm{ideal},K}$



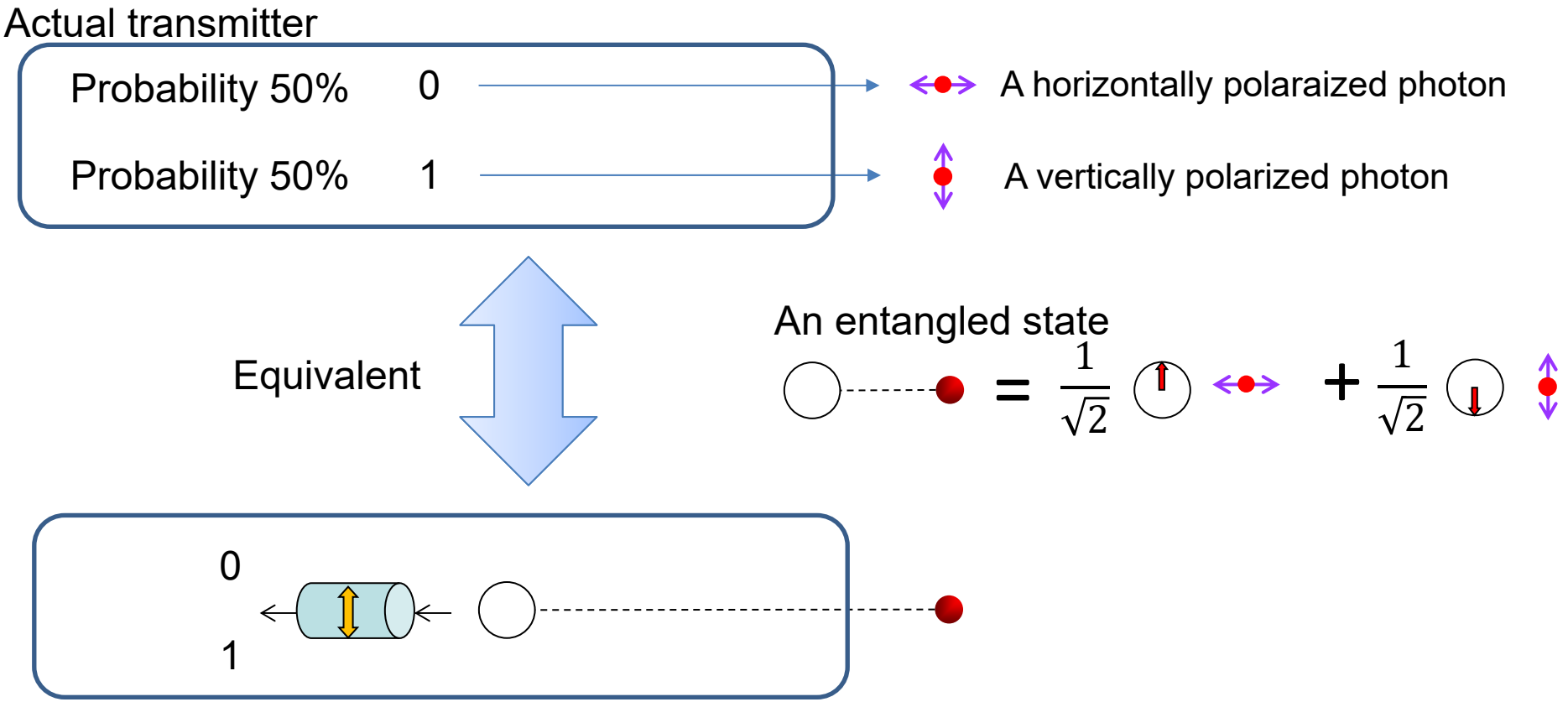
$$|+\rangle = (|0\rangle + |1\rangle)/\sqrt{2}$$

Alice: “I am a sender of optical pulses. I see no qubits in my transmitter.”

Bob: “Well, I’d be happy to see Alice’s key is secret, but the thing is, I don’t know her key either…”

Converting a sender to a receiver

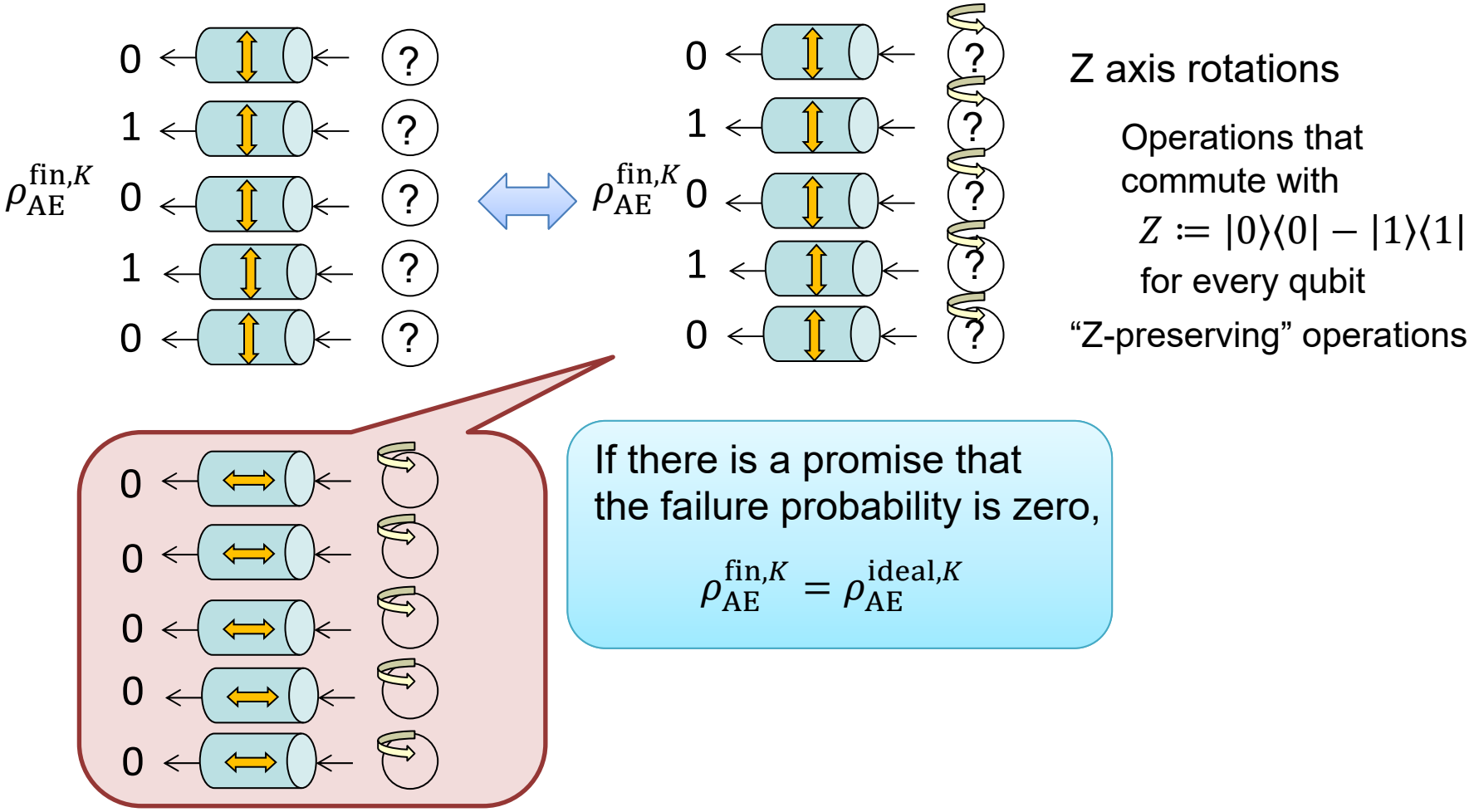
Alice: “I am a sender of optical pulses. I see no qubits in my transmitter.”



Cases with a larger number of states, mixed states, and different probabilities are the same, except that the size of virtual quantum system may be larger. Then a qubit can be defined in a security proof.

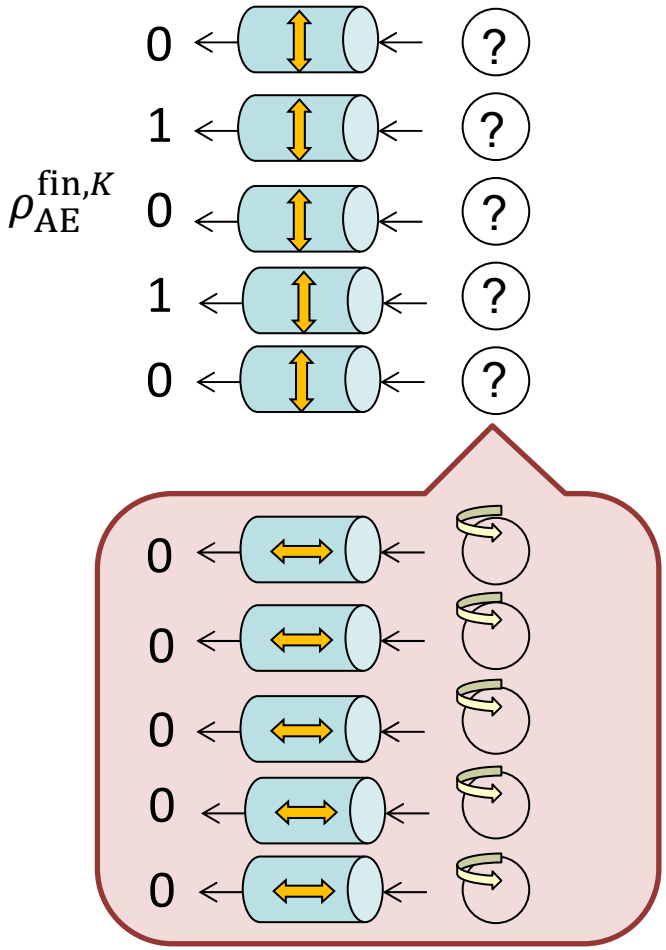
Freedom of Z rotation

Bob: “Well, I’d be happy to see Alice’s key is secret,
but the thing is, I don’t know her key either…”



Freedom of Z rotation

Bob: “Well, I’d be happy to see Alice’s key is secret,
but the thing is, I don’t know her key either…”

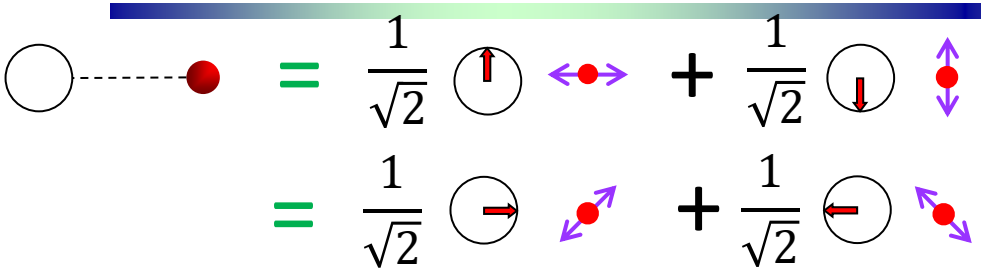


If there is a promise that
the failure probability is zero,

$$\rho_{\mathrm{AE}}^{\mathrm{fin},K} = \rho_{\mathrm{AE}}^{\mathrm{ideal},K}$$

Z axis rotations are freely allowed to decrease the failure probability.

Entanglement



Correctness

Bob

$\rho_{\mathrm{AE}}^{\mathrm{fin},K}$

0 1 0 1 0

0 1 0 1 0

Secrecy (for Alice)

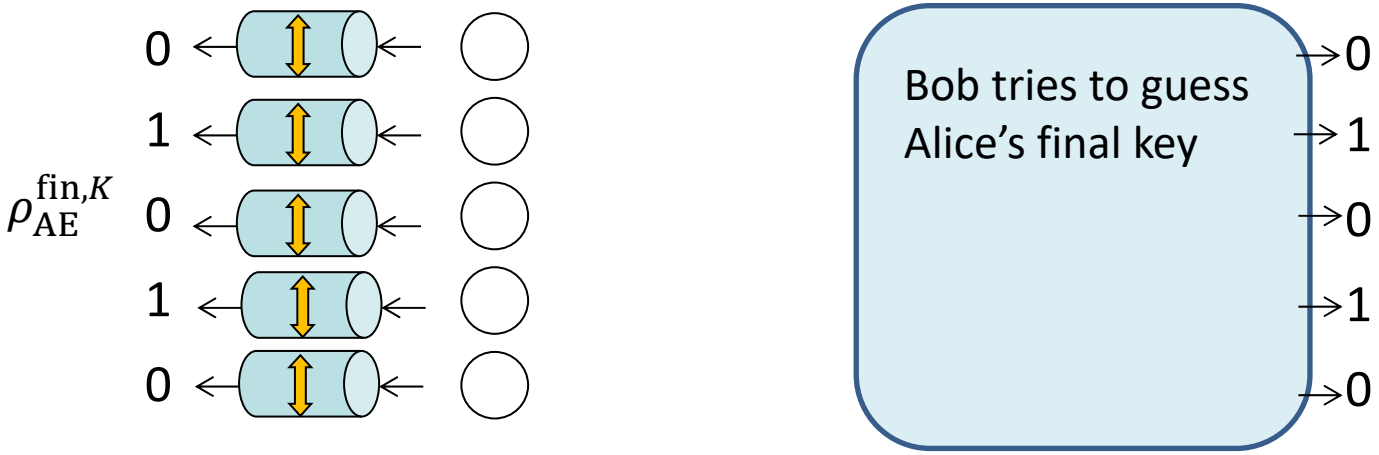
Bob

0 0 0 0 0

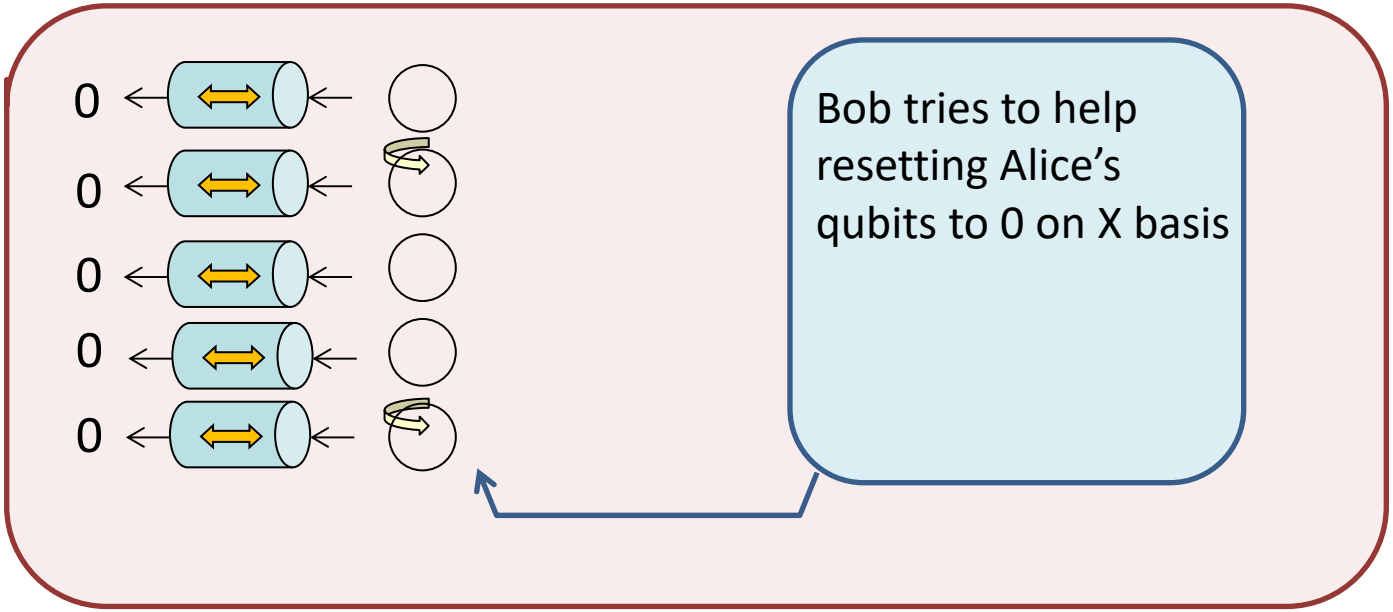
0 1 0 0 1

instruction

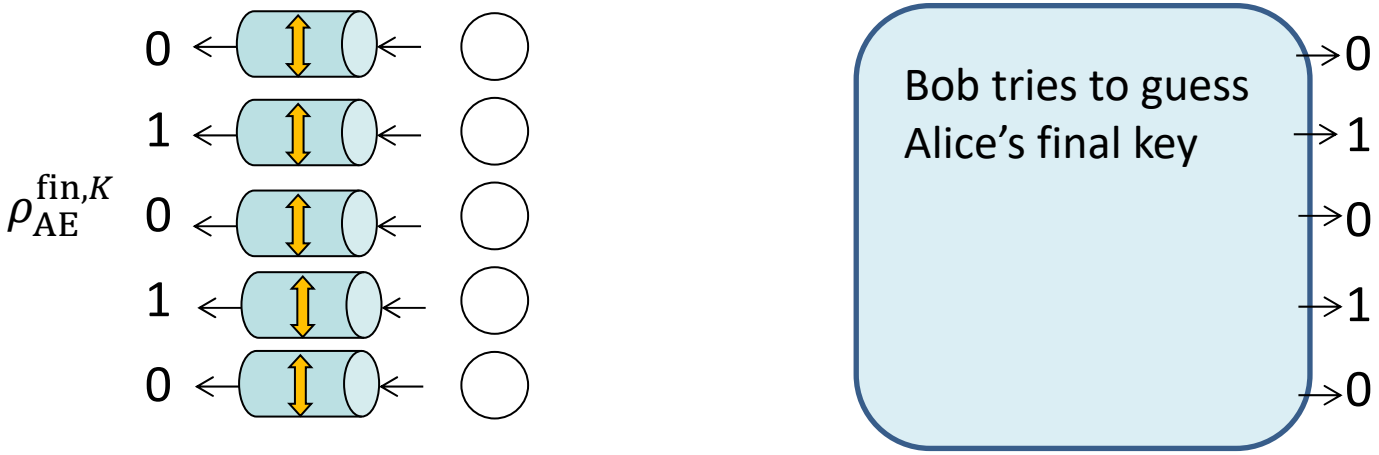
Security from complementarity



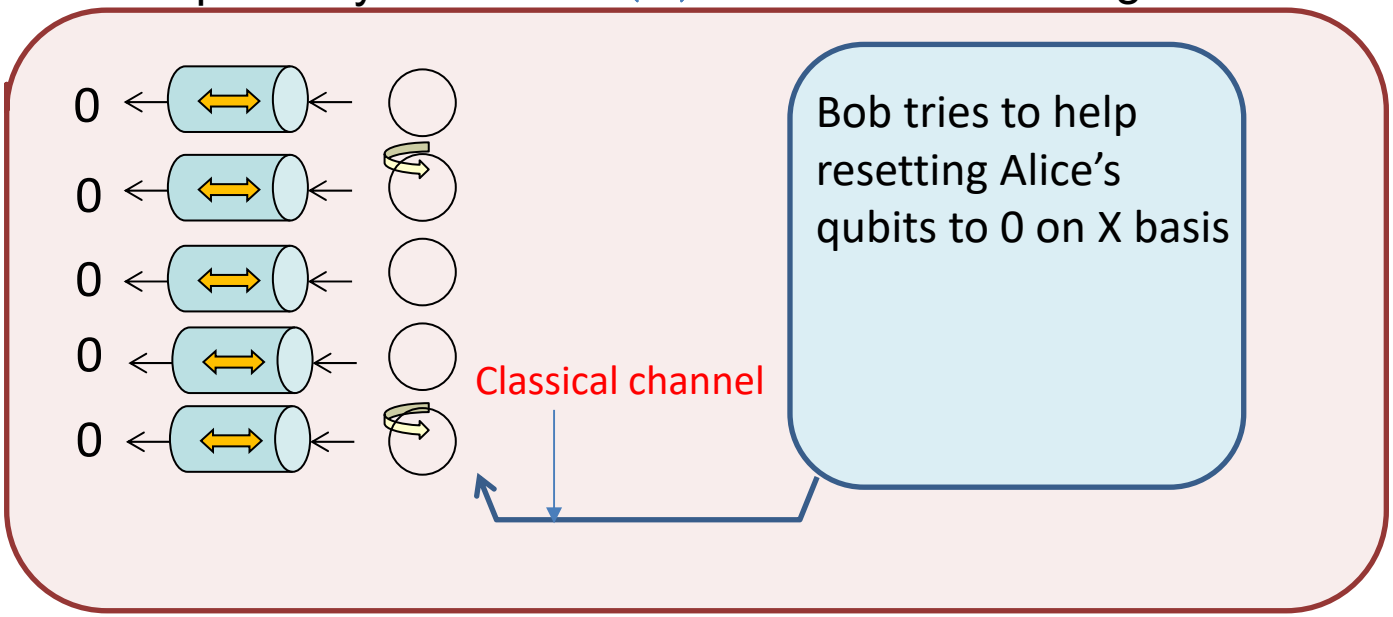
If there is a promise that the failure probability is zero, $\rho_{\mathrm{AE}}^{\mathrm{fin},K} = \rho_{\mathrm{AE}}^{\mathrm{ideal},K}$



Security from complementarity

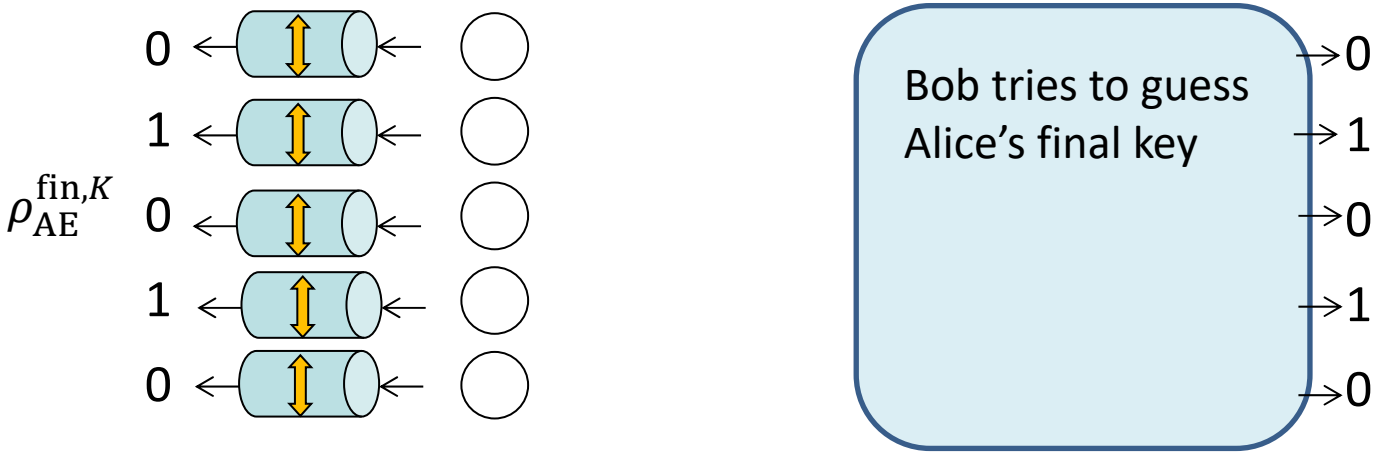


Both tasks are perfectly feasible ⟺ K ebits of entanglement

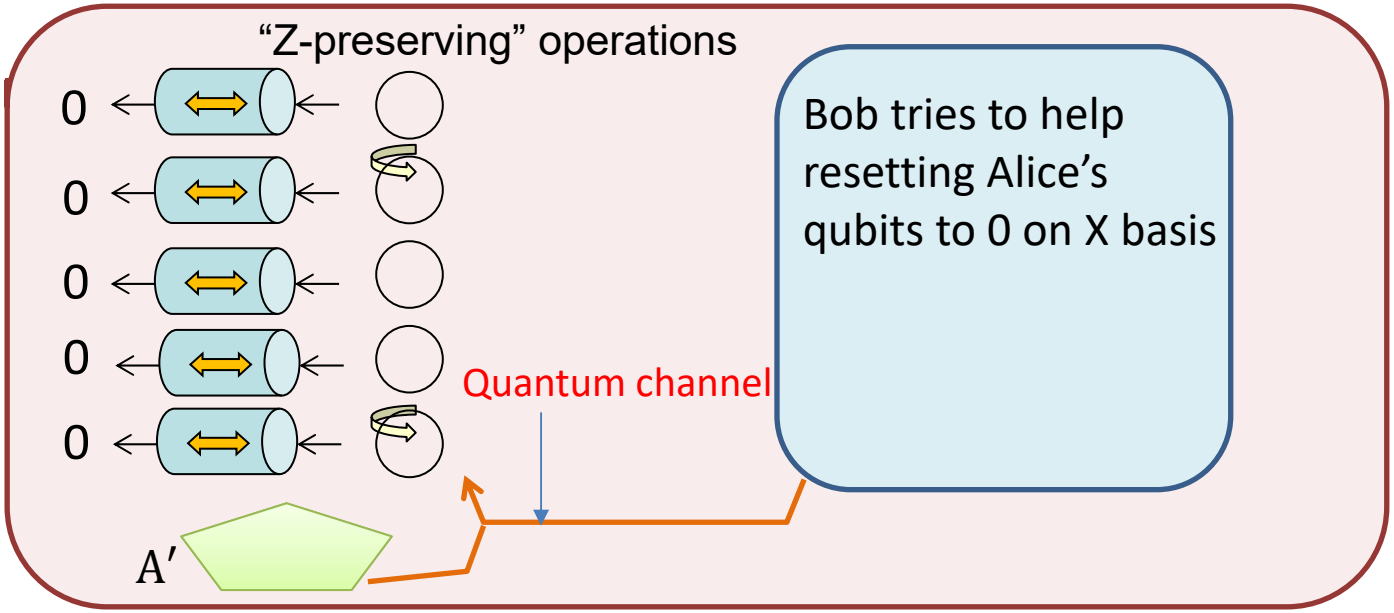


MK, arXiv:0704.3661

Security from complementarity

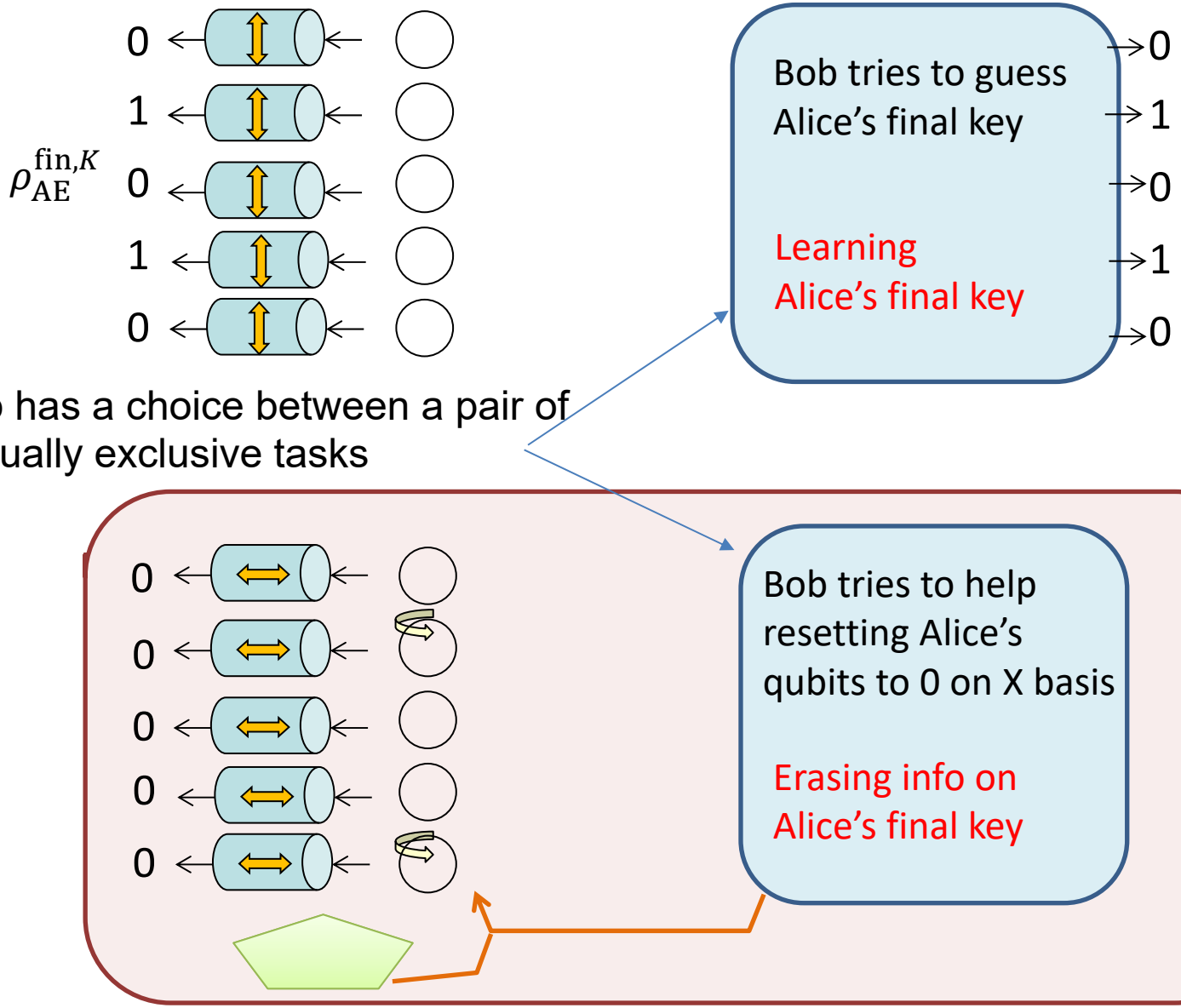


If there is a promise that the failure probability is zero, $\rho_{\mathrm{AE}}^{\mathrm{fin},K} = \rho_{\mathrm{AE}}^{\mathrm{ideal},K}$



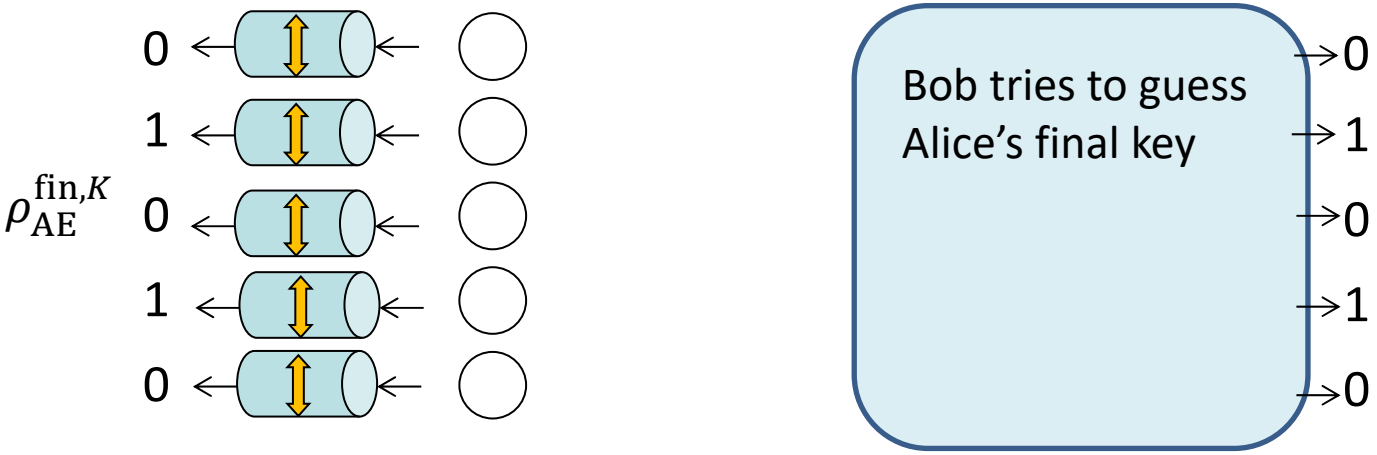
MK, *New J. Phys.*, **11**, 045018 (2009); MK, arXiv:0704.3661

Security from complementarity



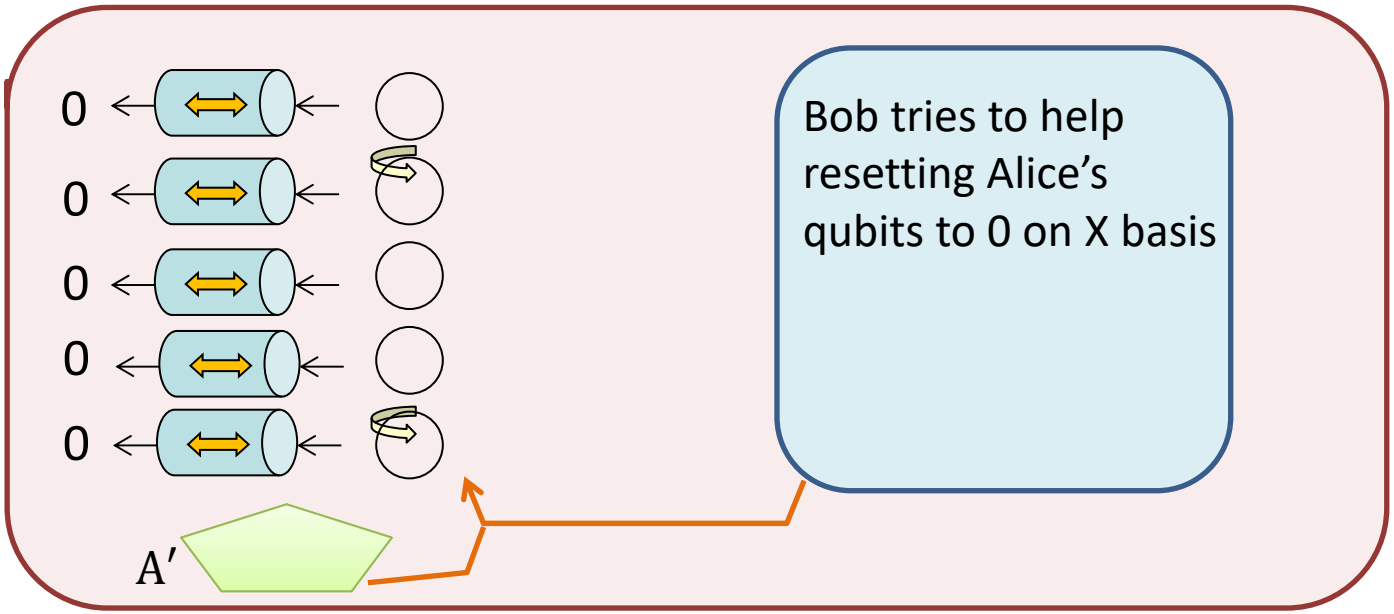
STEP 2: Almost perfect world

Small imperfection



We want a theorem looking like

If there is a promise that the failure probability is $\leq \delta$, $\rho_{\mathrm{AE}}^{\mathrm{fin},K}$ is close to $\rho_{\mathrm{AE}}^{\mathrm{ideal},K}$.



Measure of imperfection

Actual state: $\rho_{\mathrm{ABE}}^{\mathrm{fin},K} = \sum_{z,z'=0}^{2^K-1} p(z,z')|z\rangle\langle z|_{\mathrm{A}} \otimes |z'\rangle\langle z'|_{\mathrm{B}} \otimes \rho_{\mathrm{E}}(z,z')$

⇕ Proper measure of closeness?

Ideal state: $\rho_{\mathrm{ABE}}^{\mathrm{ideal},K} = \sum_{z=0}^{2^K-1} 2^{-K}|z\rangle\langle z|_{\mathrm{A}} \otimes |z\rangle\langle z|_{\mathrm{B}} \otimes \rho_{\mathrm{E}}$

A standard measure in QKD (Universal composable security)

- Use of trace distance

$$\frac{1}{2}\left\|\rho_{\mathrm{ABE}}^{\mathrm{fin},K} - \rho_{\mathrm{ABE}}^{\mathrm{ideal},K}\right\|_1 \qquad \|A\|_1 := \mathrm{Tr}\left(\sqrt{A^\dagger A}\right)$$

Monotonicity: $\|\rho-\sigma\|_1 \geq \|\Lambda(\rho)-\Lambda(\sigma)\|_1$ for any CPTP map Λ.

Triangle inequality: $\|\rho-\sigma\|_1 \leq \|\rho-\tau\|_1 + \|\tau-\sigma\|_1$

- Specification of ρ_{E}

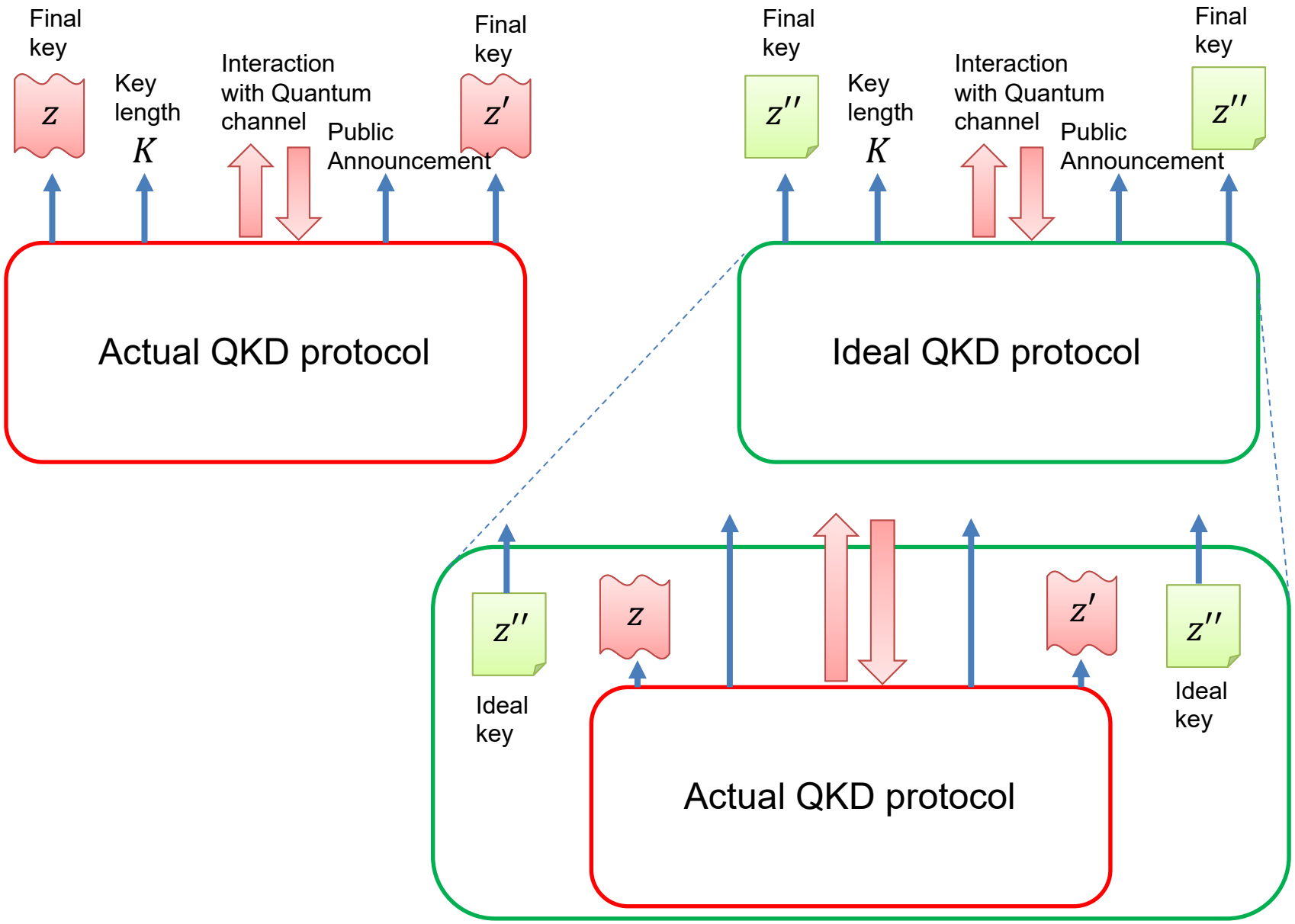
$$\rho_{\mathrm{E}} = \mathrm{Tr}_{\mathrm{AB}}\left(\rho_{\mathrm{ABE}}^{\mathrm{ideal},K}\right) = \mathrm{Tr}_{\mathrm{AB}}\left(\rho_{\mathrm{ABE}}^{\mathrm{fin},K}\right) = \sum_{z,z'=0}^{2^K-1} p(z,z')\ \rho_{\mathrm{E}}(z,z')$$

- Regard system E as 'everything', not just an adversary's system.

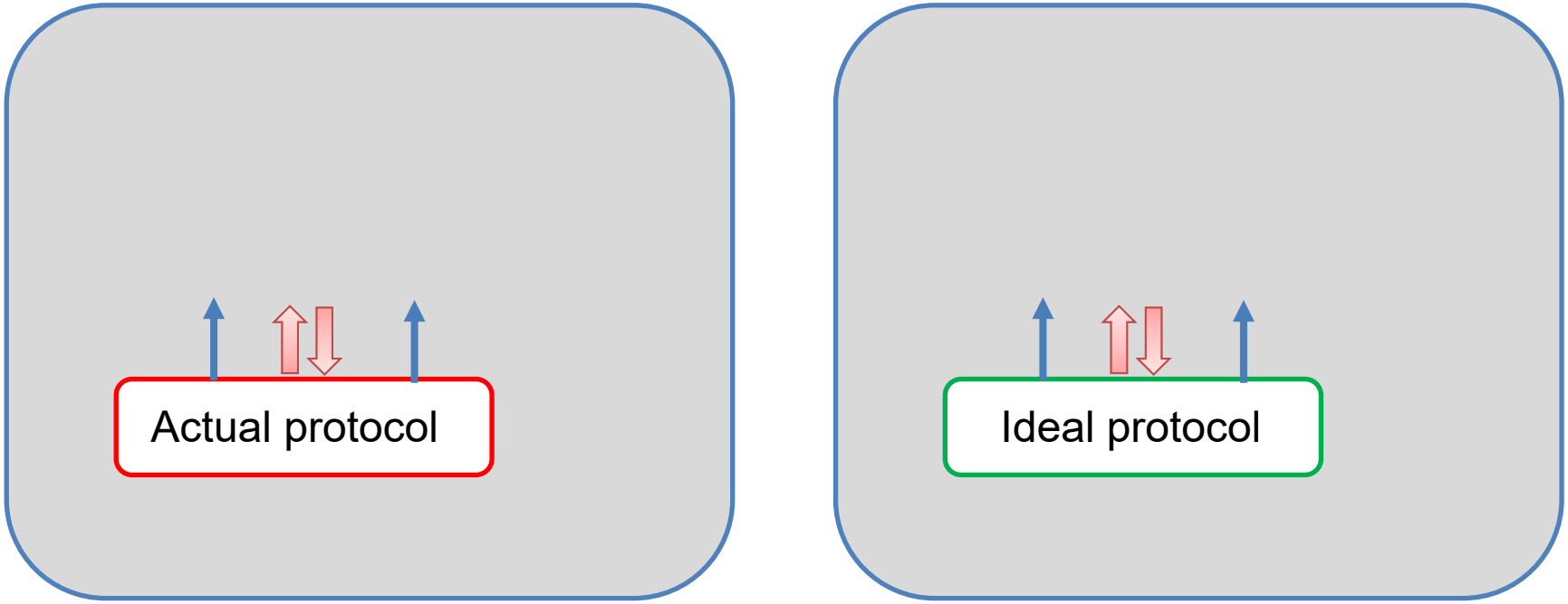
(As long as you are proving security against general attacks, you don't have to worry about this difference.)

Ben-Or, M. Horodecki, Leung, Mayers, Oppenheim, in *Proc. 2nd Theory Cryptogr. Conf.*, **3378**, 386 (2005)

Universal composable security



Universal composable security



State of the gray area: ρ^{actual} ρ^{ideal}

The protocol is ϵ-secure:

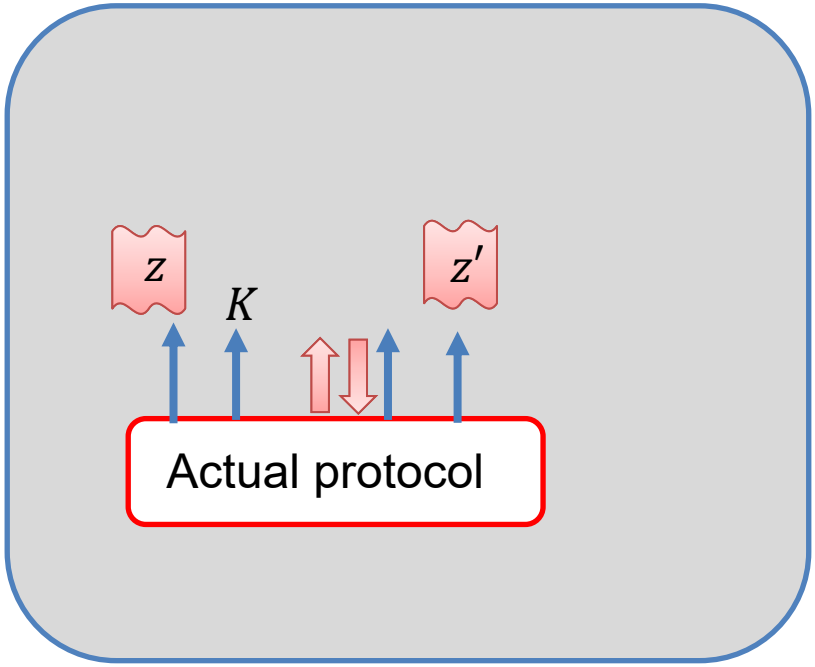
It is guaranteed that $\frac{1}{2}\left\|\rho^{\text{actual}} - \rho^{\text{ideal}}\right\|_1 \leq \epsilon$

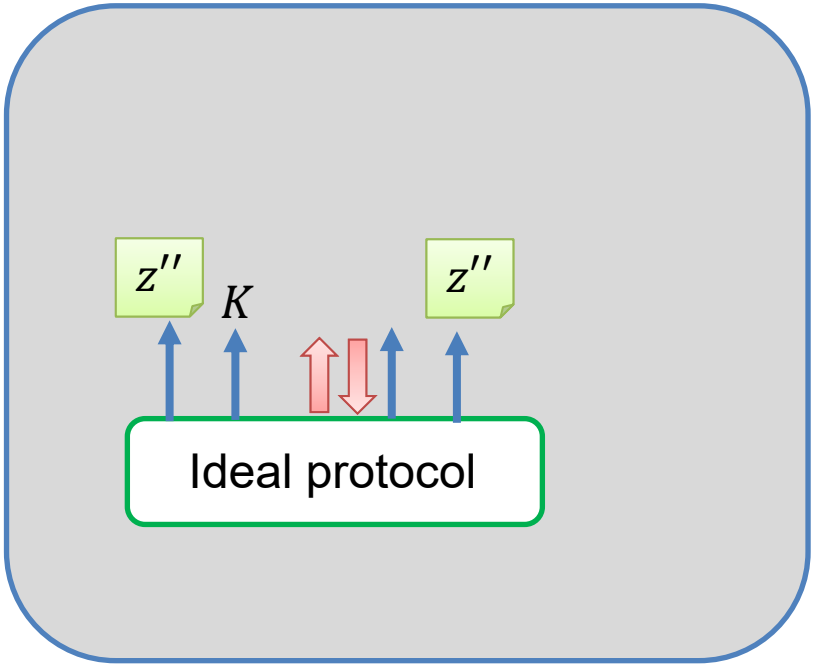
Monotonicity: $\|\rho - \sigma\|_1 \geq \|\Lambda(\rho) - \Lambda(\sigma)\|_1$

For any event in the future,

$$|\text{Prob}(event|\text{actual}) - \text{Prob}(event|\text{ideal})| \leq \epsilon$$

Universal composable security





State of the gray area: $\rho^{\text{actual}} = \langle \rho_{\text{ABE}}^{\text{fin},K} \rangle_K$

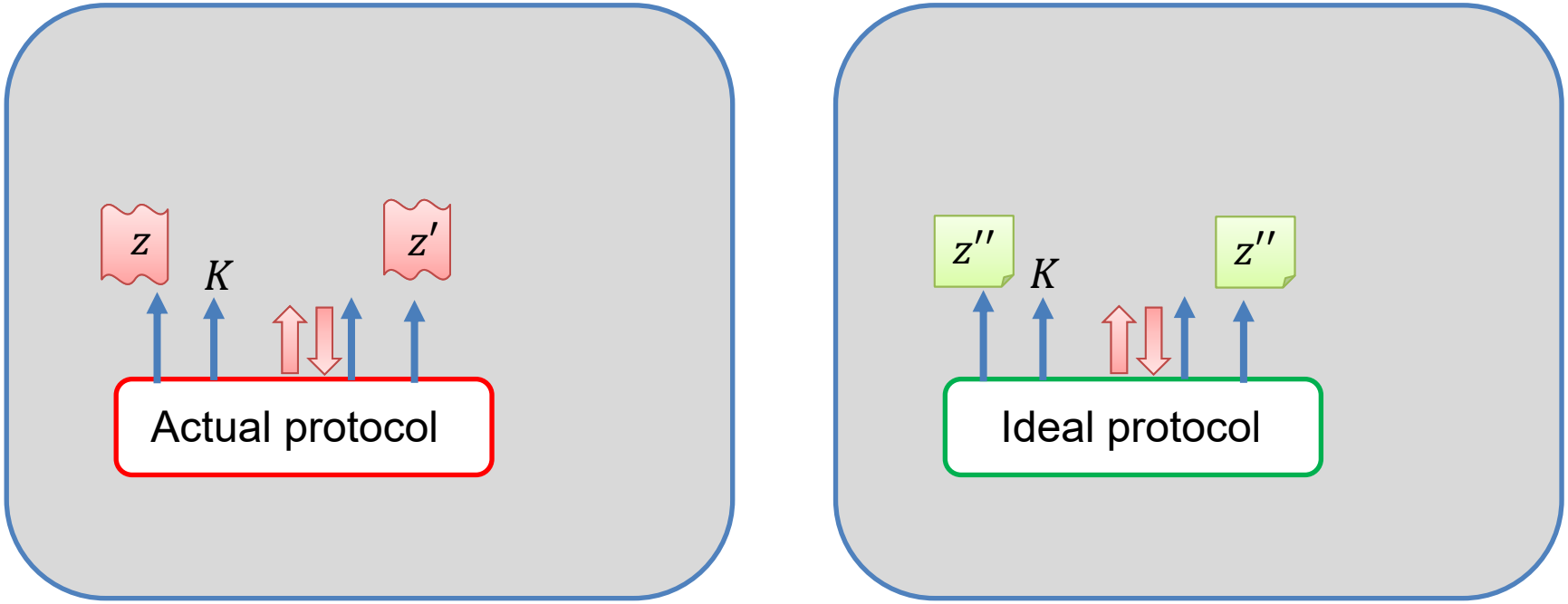
$\rho^{\text{ideal}} = \langle \rho_{\text{ABE}}^{\text{ideal},K} \rangle_K$

$$\rho_{\text{ABE}}^{\text{fin},K} = \sum_{z,z'=0}^{2^K-1} p(z,z') |z\rangle\langle z|_{\text{A}} \otimes |z'\rangle\langle z'|_{\text{B}} \otimes \rho_{\text{E}}(z,z')$$

$$\sum_{z''=0}^{2^K-1} 2^{-K} |z''\rangle\langle z''|_{\text{A}} \otimes |z''\rangle\langle z''|_{\text{B}} \otimes \sum_{z,z'=0}^{2^K-1} p(z,z')\, \rho_{\text{E}}(z,z') = \rho_{\text{ABE}}^{\text{ideal},K}$$

$$\text{Tr}_{\text{AB}}\left(\rho_{\text{ABE}}^{\text{ideal},K}\right) = \text{Tr}_{\text{AB}}\left(\rho_{\text{ABE}}^{\text{fin},K}\right)$$

Universal composable security



State of the gray area: $\rho^{\text{actual}} = \langle \rho_{\text{ABE}}^{\text{fin},K} \rangle_K$

$\rho^{\text{ideal}} = \langle \rho_{\text{ABE}}^{\text{ideal},K} \rangle_K$

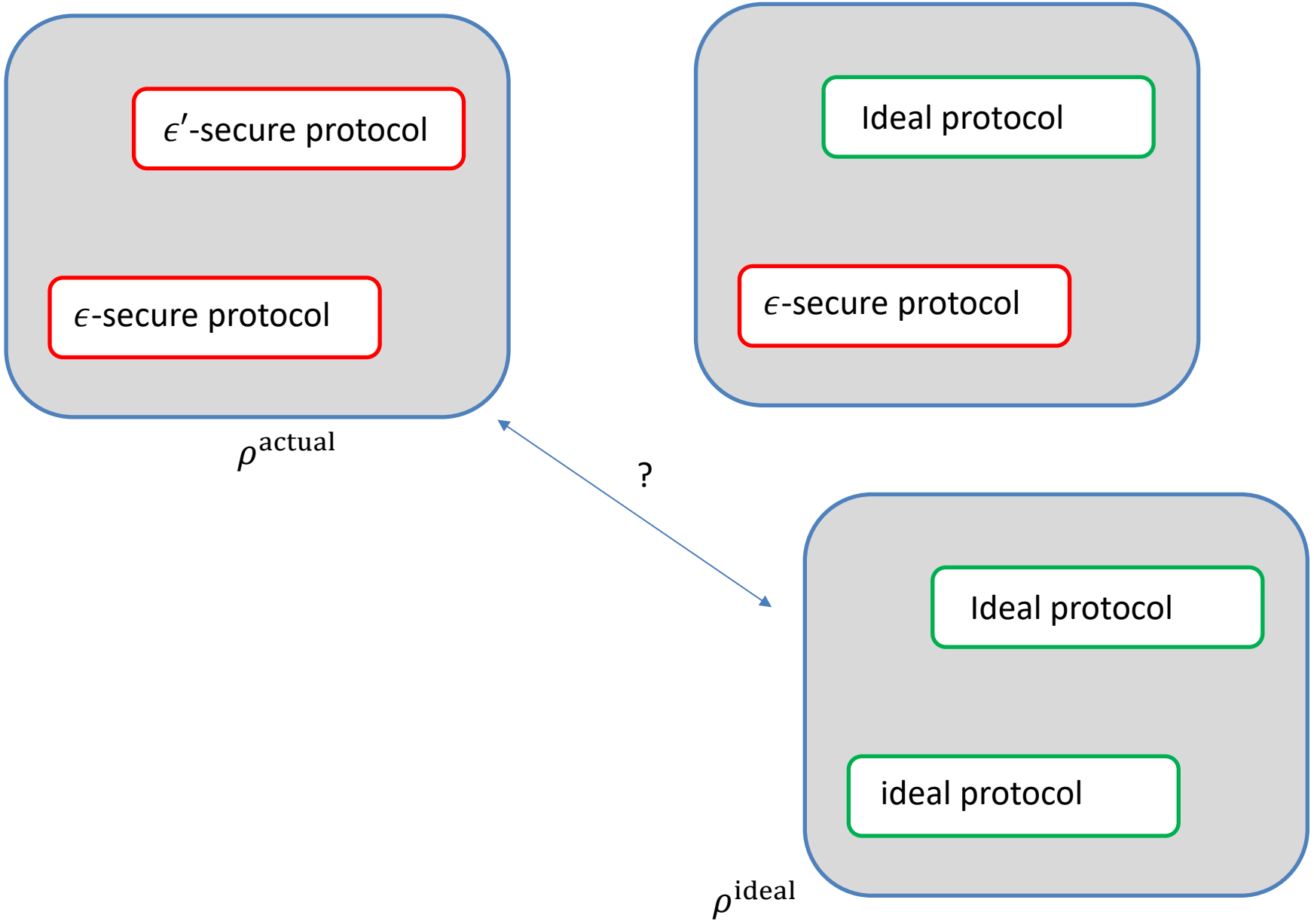
A QKD protocol is ϵ-secure if

$$\left\langle \frac{1}{2} \left\| \rho_{\text{ABE}}^{\text{fin},K} - \rho_{\text{ABE}}^{\text{ideal},K} \right\|_1 \right\rangle_K \leq \epsilon$$

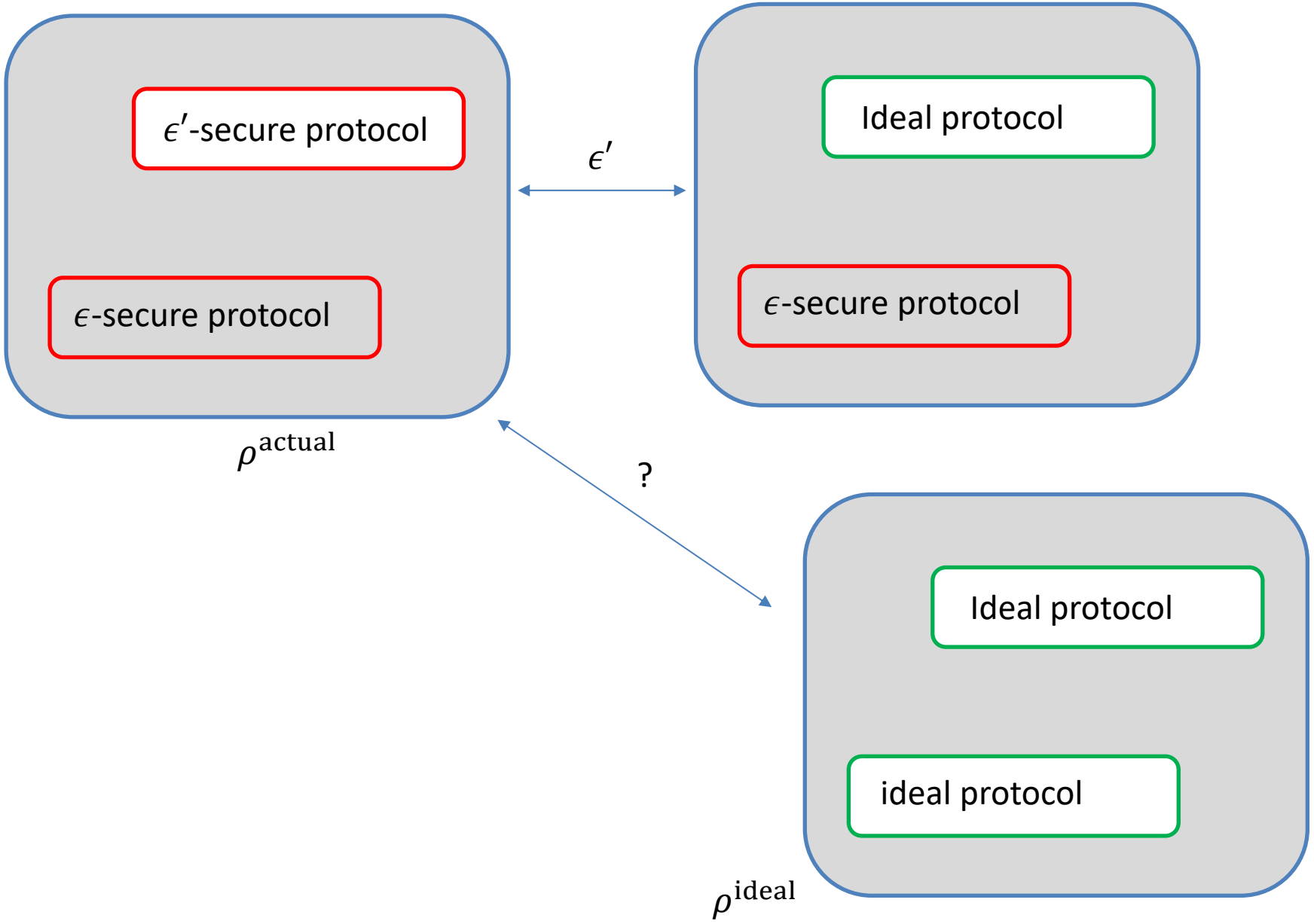
VI

$$\frac{1}{2} \left\| \langle \rho_{\text{ABE}}^{\text{fin},K} \rangle_K - \langle \rho_{\text{ABE}}^{\text{ideal},K} \rangle_K \right\|_1$$

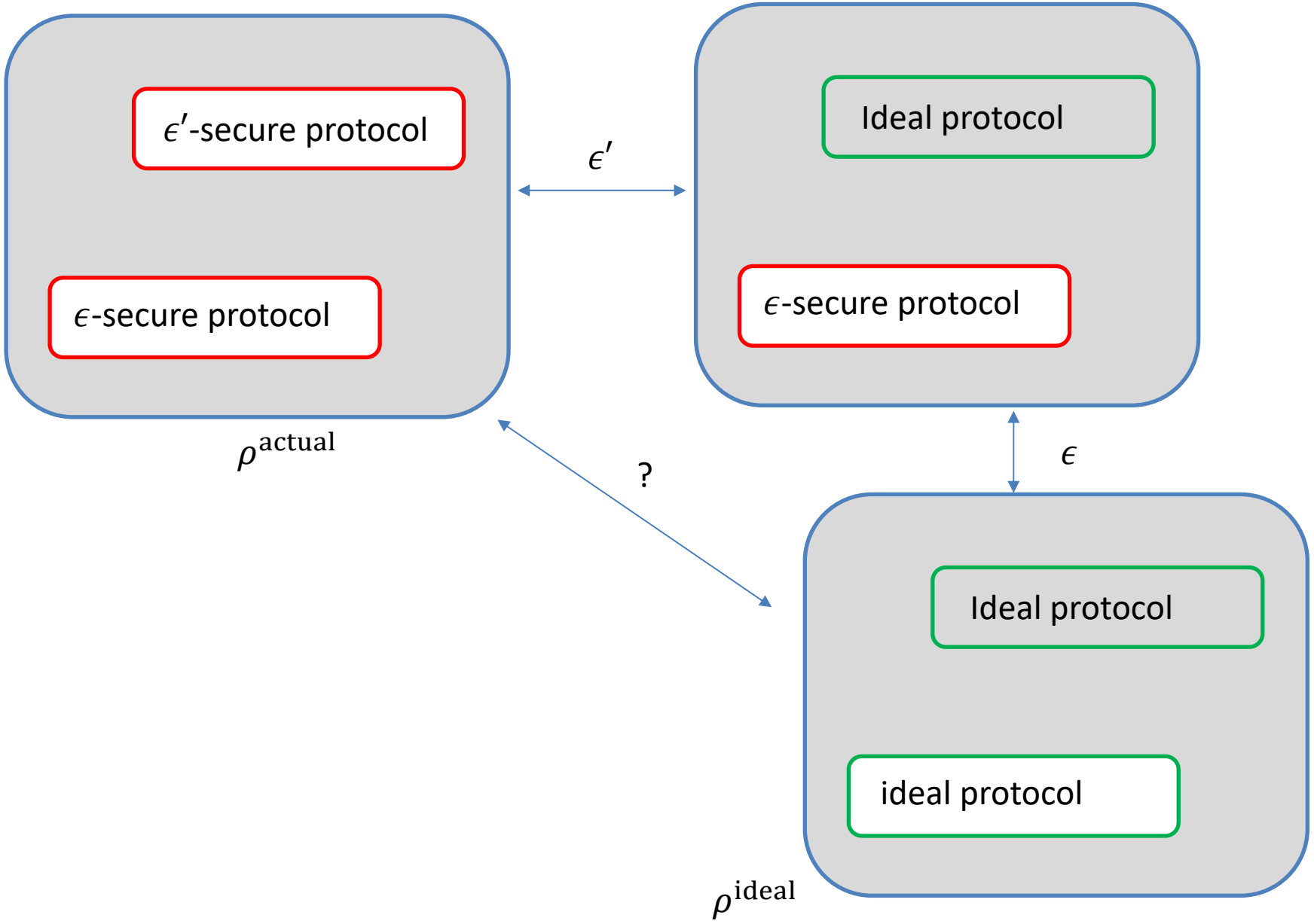
Universal composable security



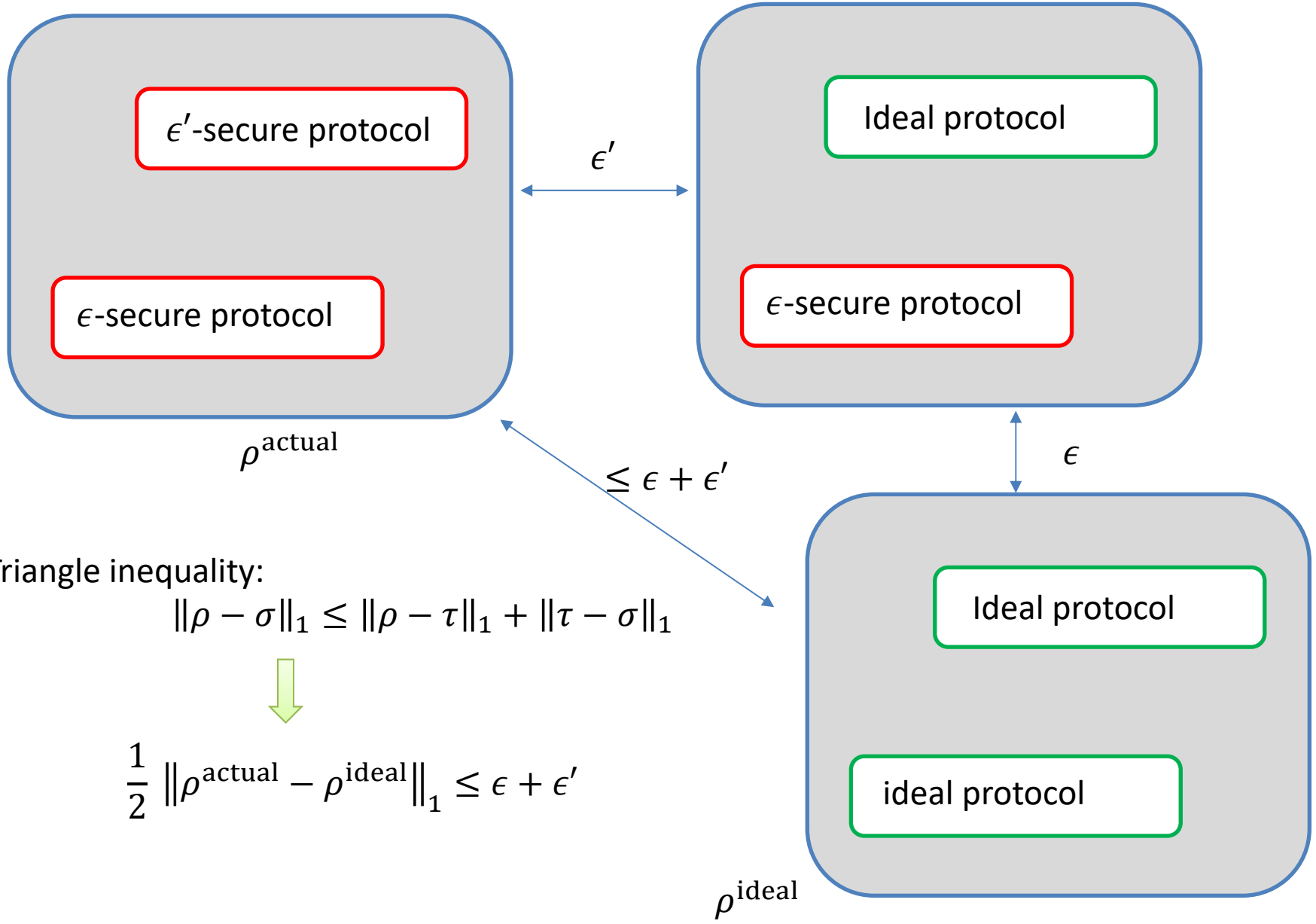
Universal composable security



Universal composable security



Universal composable security



Triangle inequality:

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

$$\frac{1}{2} \left\|\rho^{\text{actual}} - \rho^{\text{ideal}}\right\|_1 \leq \epsilon + \epsilon'$$

Dividing the requirement

Imperfection of the final key

Overall security

(ϵ-secure) $\left\langle \frac{1}{2} \left\| \rho_{\mathrm{ABE}}^{\mathrm{fin},K} - \rho_{\mathrm{ABE}}^{\mathrm{ideal},K} \right\|_1 \right\rangle_K \leq \epsilon$

With $\epsilon = \epsilon' + \epsilon''$

Secrecy (for Alice)

$\left\langle \frac{1}{2} \left\| \rho_{\mathrm{AE}}^{\mathrm{fin},K} - \rho_{\mathrm{AE}}^{\mathrm{ideal},K} \right\|_1 \right\rangle_K \leq \epsilon'$ (ϵ'-secret)

Correctness

$\mathrm{Prob}(z \neq z') \leq \epsilon''$ (ϵ''-correct)

$$\rho_{\mathrm{AE}}^{\mathrm{fin},K} = \sum_{z=0}^{2^K-1} p(z)|z\rangle\langle z|_{\mathrm{A}} \otimes \rho_{\mathrm{E}}(z)$$

ϵ'

$$\rho_{\mathrm{AE}}^{\mathrm{ideal},K} = \sum_{z=0}^{2^K-1} 2^{-K}|z\rangle\langle z|_{\mathrm{A}} \otimes \rho_{\mathrm{E}}$$

$$\rho_{\mathrm{ABE}}^{\mathrm{fin},K} = \sum_{z,z'=0}^{2^K-1} p(z,z')|z\rangle\langle z|_{\mathrm{A}} \otimes |z'\rangle\langle z'|_{\mathrm{B}} \otimes \rho_{\mathrm{E}}(z,z')$$

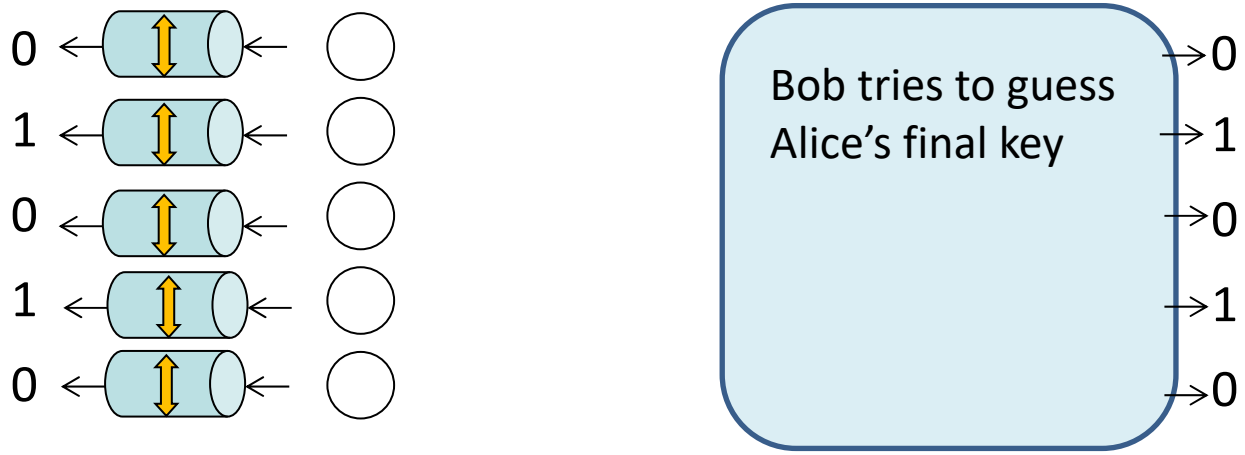
ϵ''

$$\sum_{z,z'=0}^{2^K-1} p(z,z')|z\rangle\langle z|_{\mathrm{A}} \otimes |z\rangle\langle z|_{\mathrm{B}} \otimes \rho_{\mathrm{E}}(z,z')$$

ϵ'

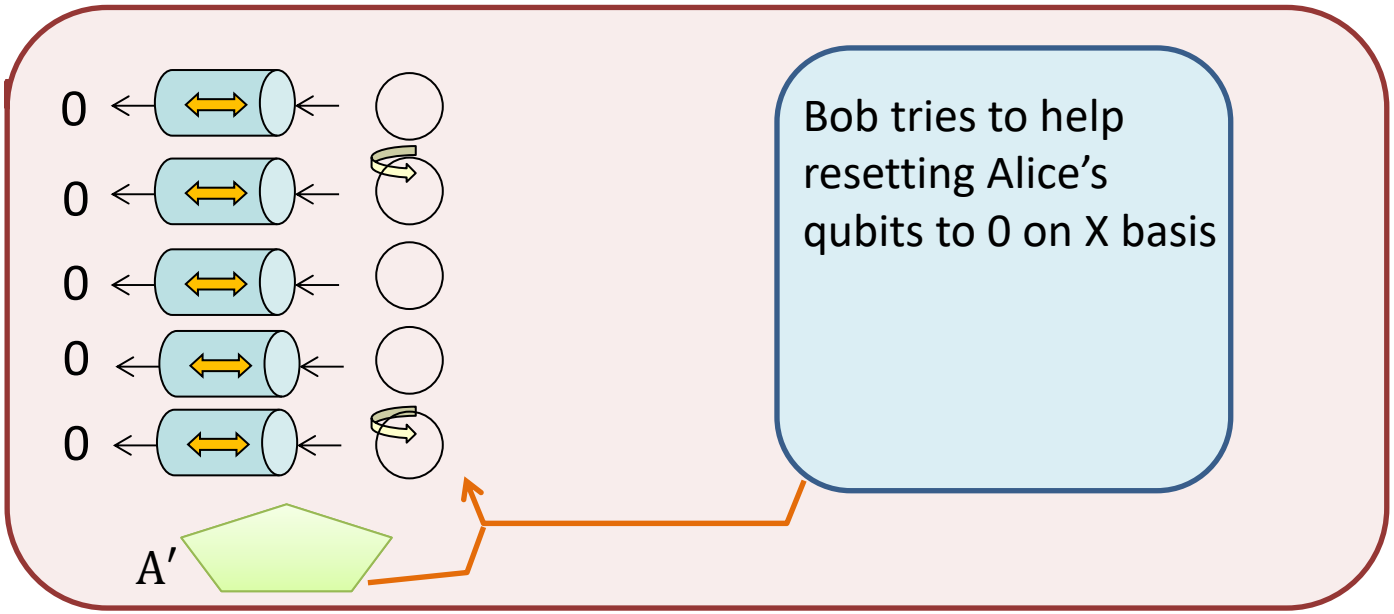
$$\rho_{\mathrm{ABE}}^{\mathrm{ideal},K} = \sum_{z=0}^{2^K-1} 2^{-K}|z\rangle\langle z|_{\mathrm{A}} \otimes |z\rangle\langle z|_{\mathrm{B}} \otimes \rho_{\mathrm{E}}$$

Small imperfection



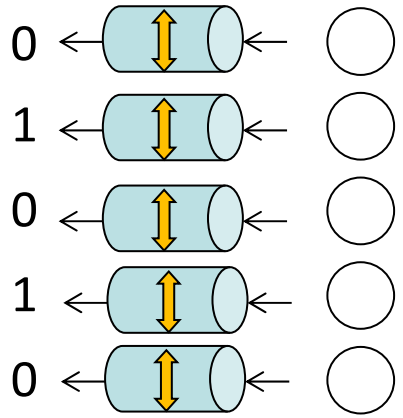
We want a theorem looking like

If there is a promise that the failure probability is $\leq \delta$, the protocol is ϵ-secret.

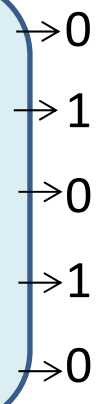


Small imperfection

$\sqrt{2\delta}$-secret

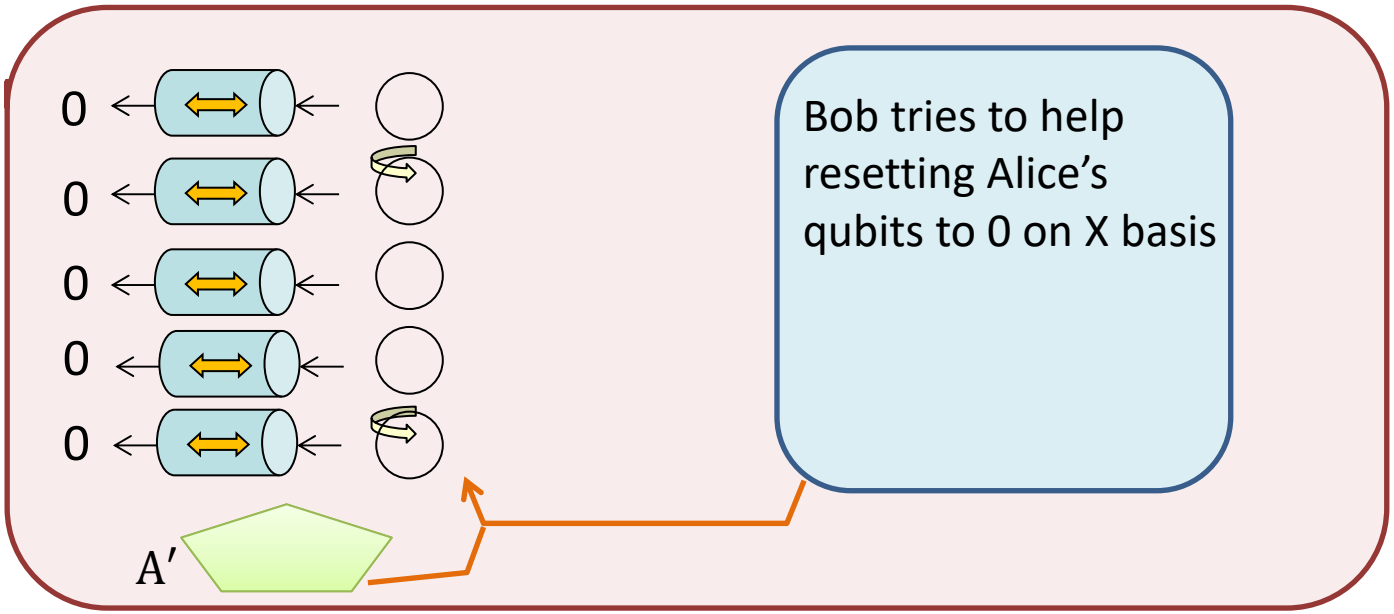


Bob tries to guess Alice's final key



If there is a promise that the failure probability is $\leq \delta$, the protocol is $\sqrt{2\delta}$-secret.

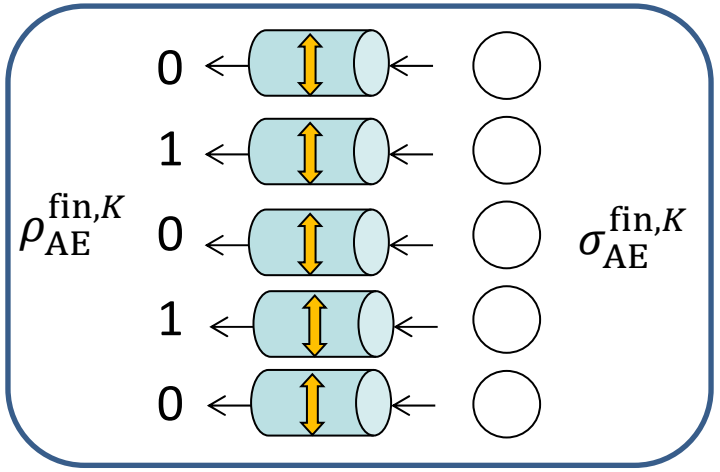
Failure$\leq \delta$

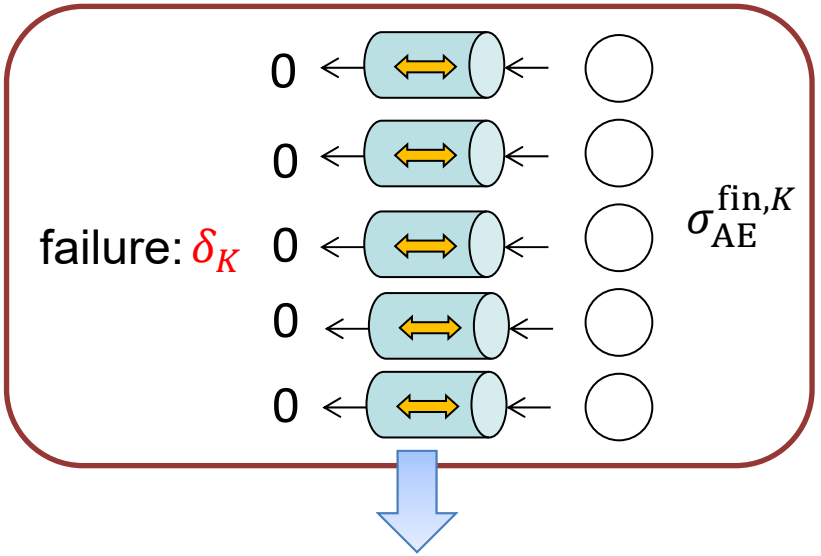


Relation between failure probability and secrecy

$$\rho_{\mathrm{E}} := \mathrm{Tr}_{\mathrm{A}}\left(\rho_{\mathrm{AE}}^{\mathrm{fin},K}\right) = \mathrm{Tr}_{\mathrm{A}}\left(\sigma_{\mathrm{AE}}^{\mathrm{fin},K}\right)$$

$$|\varphi\rangle_{\mathrm{AEE}'} \xrightarrow{\mathrm{Tr}_{\mathrm{E}'}} \sigma_{\mathrm{AE}}^{\mathrm{fin},K} \xrightarrow{\mathrm{Tr}_{\mathrm{A}}} \rho_{\mathrm{E}}$$

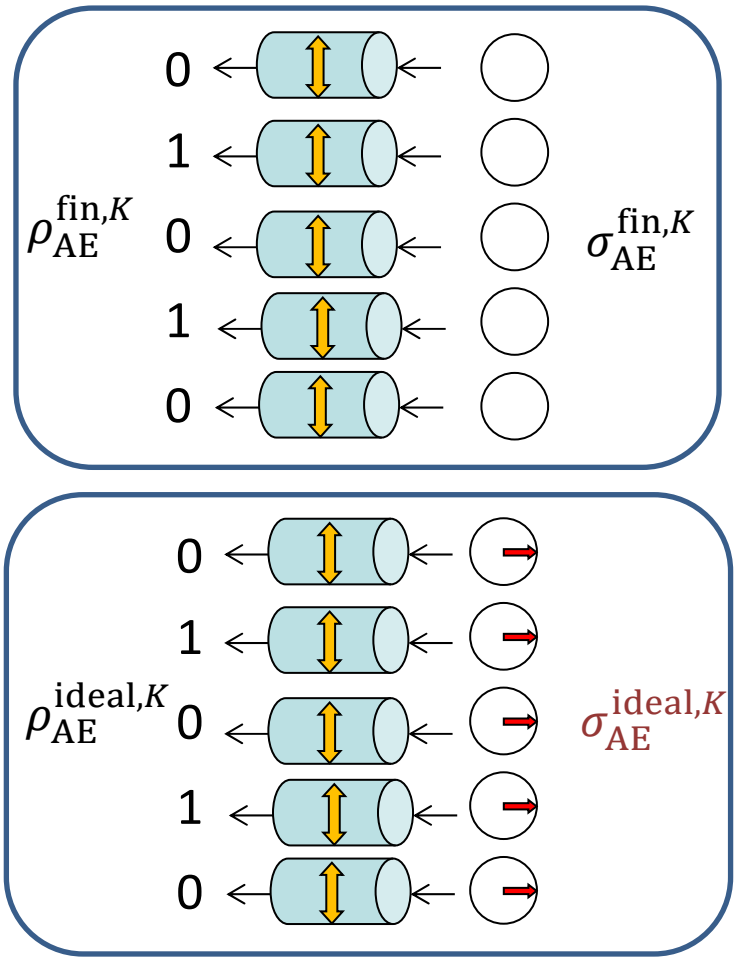




$$1-\delta_K = \mathrm{Tr}_{\mathrm{E}}\ {}_{\mathrm{A}}\langle +^K|\, \sigma_{\mathrm{AE}}^{\mathrm{fin},K}\, |+^K\rangle_{\mathrm{A}} = {}_{\mathrm{AEE}'}\langle\varphi|\,|+^K\rangle_{\mathrm{A}}\,{}_{\mathrm{A}}\langle +^K|\,|\varphi\rangle_{\mathrm{AEE}'}$$

Hayashi, Tsurumaru, *New J. Phys.*, **14**, 093014 (2012).

Relation between failure probability and secrecy



$$\rho_E = \mathrm{Tr}_A(\rho_{AE}^{fin,K})$$

$$|\varphi\rangle_{AEE'} \xrightarrow{\mathrm{Tr}_{E'}} \sigma_{AE}^{fin,K} \xrightarrow{\mathrm{Tr}_A} \rho_E$$

$$\sigma_{AE}^{ideal,K} \eqqcolon |+^K\rangle_A\,{}_A\langle +^K| \otimes \rho_E$$

$$|\Phi\rangle_{AA'EE'} \coloneqq |+^K\rangle_A\,|\varphi\rangle_{A'EE'} \xrightarrow{\mathrm{Tr}_{A'E'}} \sigma_{AE}^{ideal,K}$$

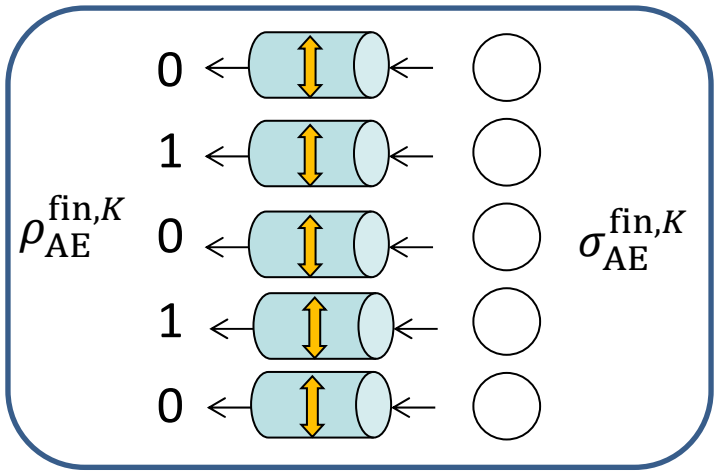
$$|\Psi\rangle_{AA'EE'} \coloneqq |\varphi\rangle_{AEE'}\,|+^K\rangle_{A'} \xrightarrow{\mathrm{Tr}_{A'E'}} \sigma_{AE}^{fin,K}$$

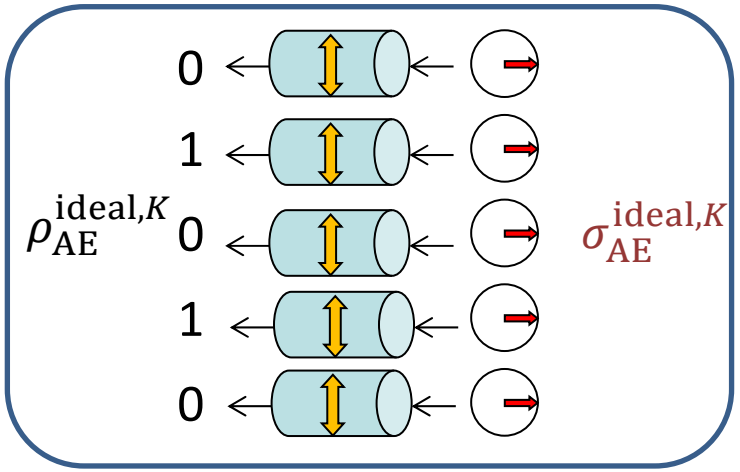
$$\langle\Phi|\Psi\rangle = {}_{A'EE'}\langle\varphi|\,|+^K\rangle_{A'}\,{}_A\langle +^K|\,|\varphi\rangle_{AEE'}$$
$$\geq 1-\delta_K$$

$$1-\delta_K = \mathrm{Tr}_E\,{}_A\langle +^K|\,\sigma_{AE}^{fin,K}\,|+^K\rangle_A = {}_{AEE'}\langle\varphi|\,|+^K\rangle_A\,{}_A\langle +^K|\,|\varphi\rangle_{AEE'}$$

Hayashi, Tsurumaru, *New J. Phys.*, **14**, 093014 (2012).

Relation between failure probability and secrecy





$$\rho_E = \mathrm{Tr}_A(\rho_{AE}^{fin,K})$$

$$|\varphi\rangle_{AEE'} \xrightarrow{\mathrm{Tr}_{E'}} \sigma_{AE}^{fin,K} \xrightarrow{\mathrm{Tr}_A} \rho_E$$

$$\sigma_{AE}^{ideal,K} \coloneqq |+^K\rangle_A\,{}_A\langle +^K| \otimes \rho_E$$

$$|\Phi\rangle_{AA'EE'} \coloneqq |+^K\rangle_A\,|\varphi\rangle_{A'EE'} \xrightarrow{\mathrm{Tr}_{A'E'}} \sigma_{AE}^{ideal,K}$$

$$|\Psi\rangle_{AA'EE'} \coloneqq |\varphi\rangle_{AEE'}\,|+^K\rangle_{A'} \xrightarrow{\mathrm{Tr}_{A'E'}} \sigma_{AE}^{fin,K}$$

$$\langle\Phi|\Psi\rangle = {}_{A'EE'}\langle\varphi|\,|+^K\rangle_{A'}\,{}_A\langle +^K|\varphi\rangle_{AEE'} \geq 1-\delta_K$$

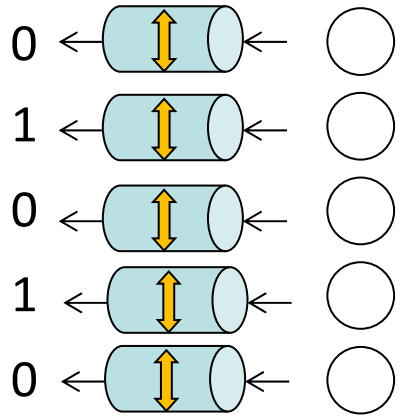
$$F(\sigma_{AE}^{fin,K}, \sigma_{AE}^{ideal,K}) \geq |\langle\Phi|\Psi\rangle|^2 \geq (1-\delta_K)^2 \geq 1-2\delta_K$$

$$\frac{1}{2}\left\|\rho_{AE}^{fin,K} - \rho_{AE}^{ideal,K}\right\|_1 \leq \sqrt{1-F} \leq \sqrt{2\delta_K} \qquad \left\langle\sqrt{2\delta_K}\right\rangle_K \leq \sqrt{2\langle\delta_K\rangle_K} \leq \sqrt{2\delta}$$

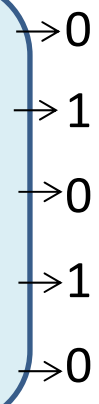
Hayashi, Tsurumaru, *New J. Phys.*, **14**, 093014 (2012).

Small imperfection

$\sqrt{2\delta}$-secret

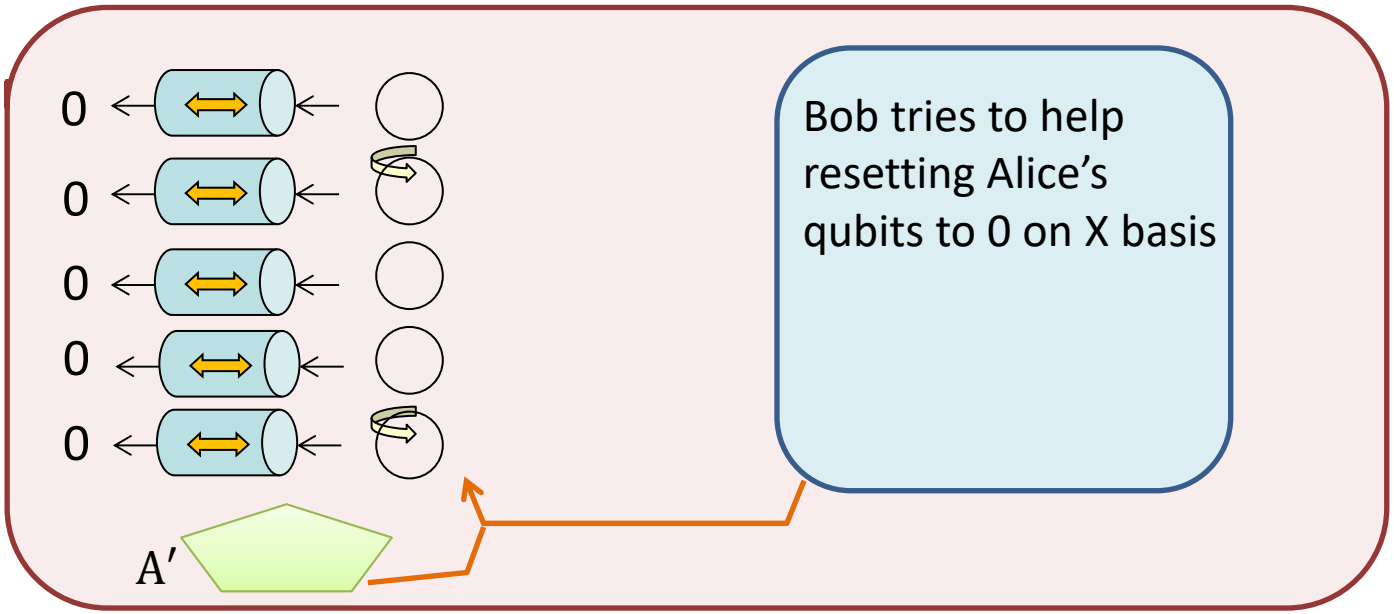


Bob tries to guess Alice's final key



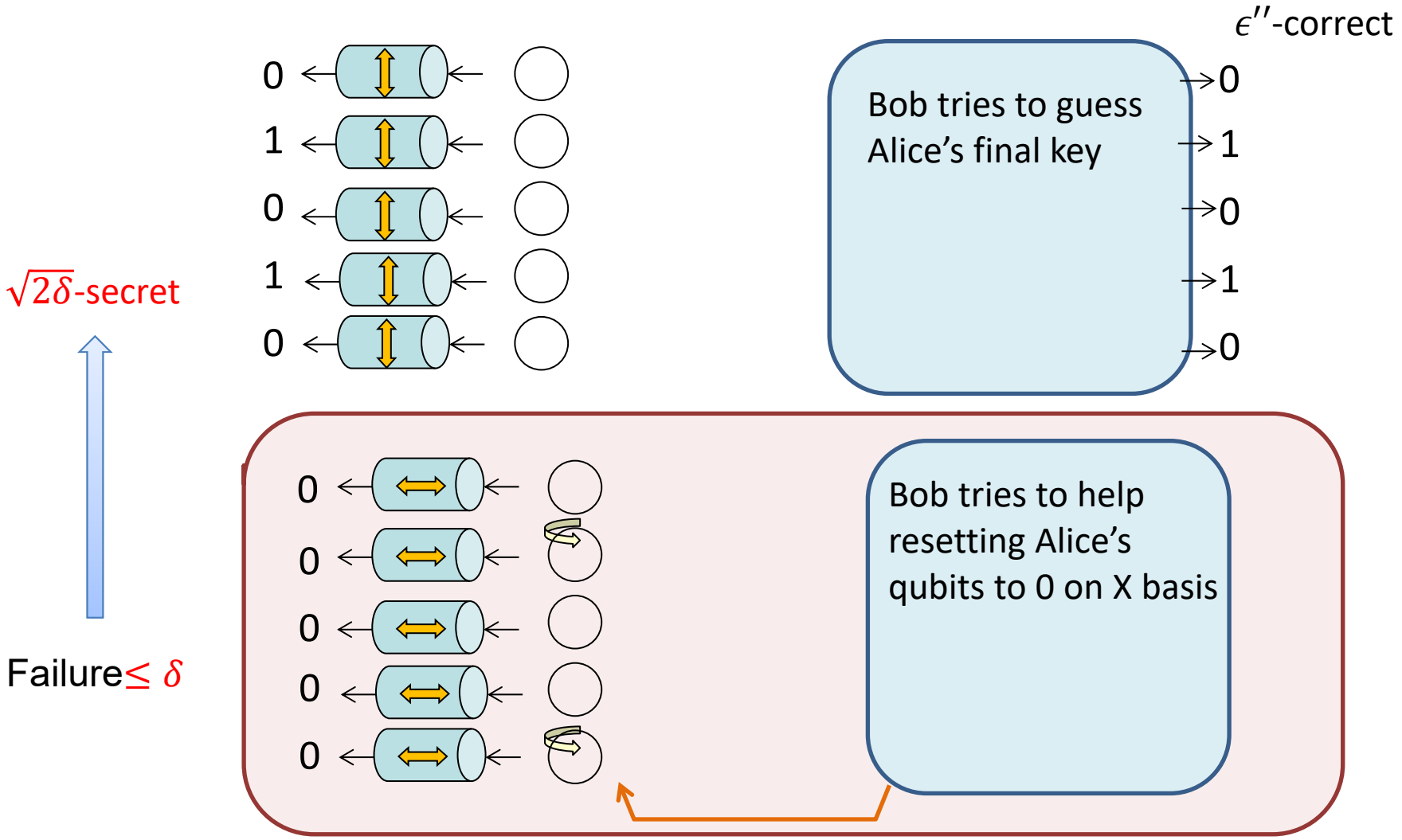
If there is a promise that the failure probability is $\leq \delta$, the protocol is $\sqrt{2\delta}$-secret.

Failure$\leq \delta$



STEP 3: Practical world

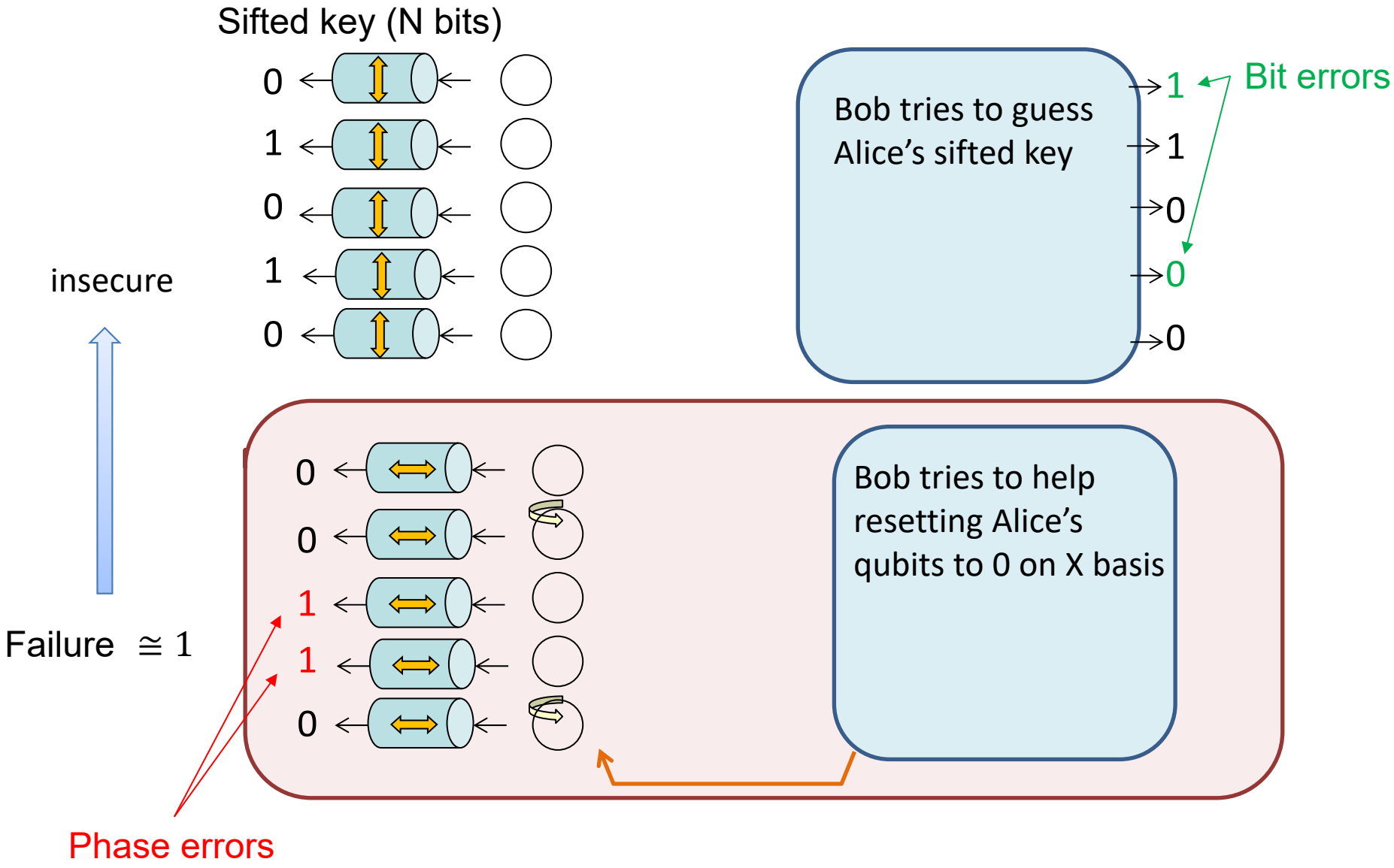
Small imperfection



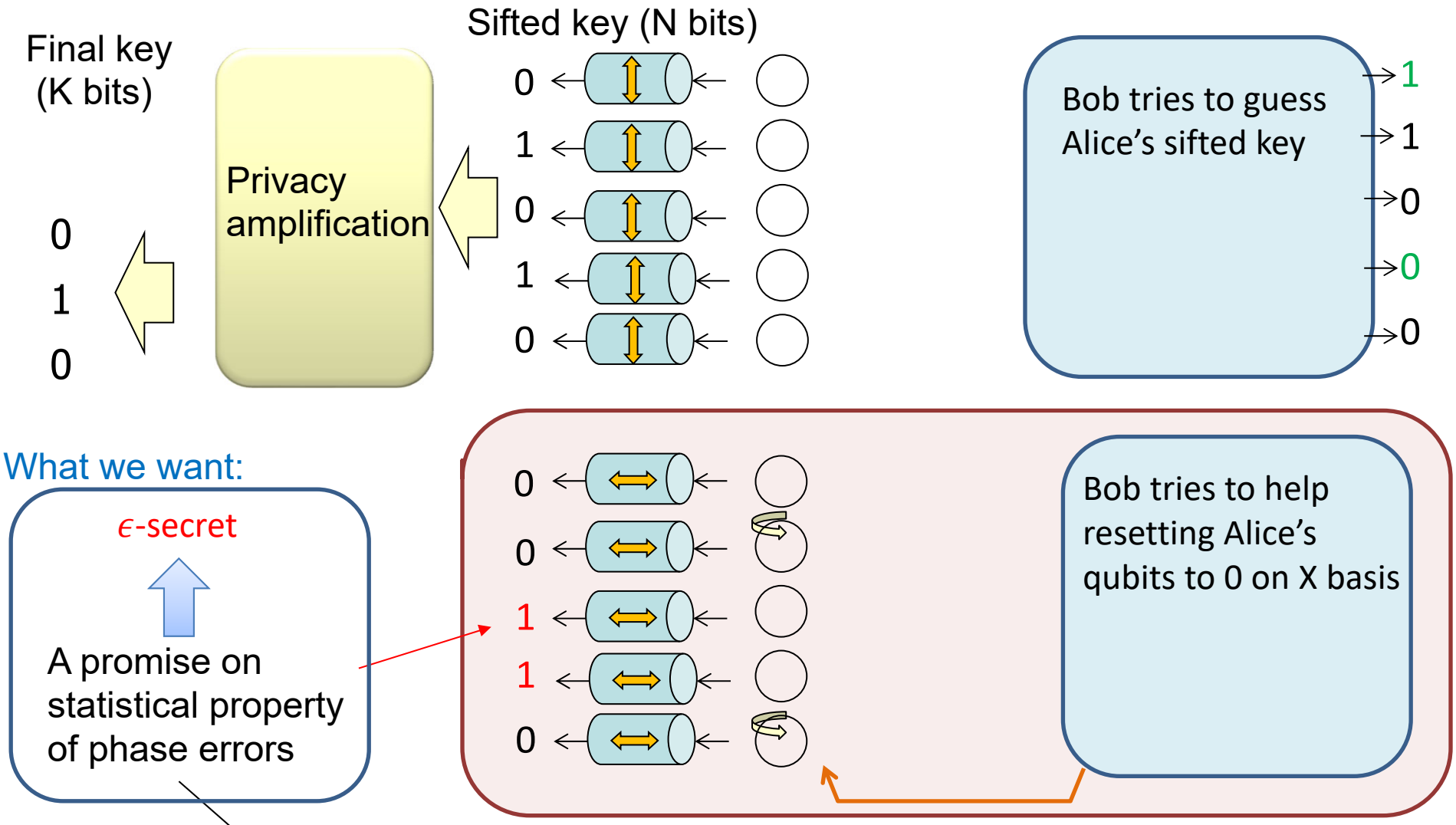
This scenario works if entanglement distillation is actually carried out.

Lo, Chau, *Science*, **283**, 2050 (1999).

Realistic cases

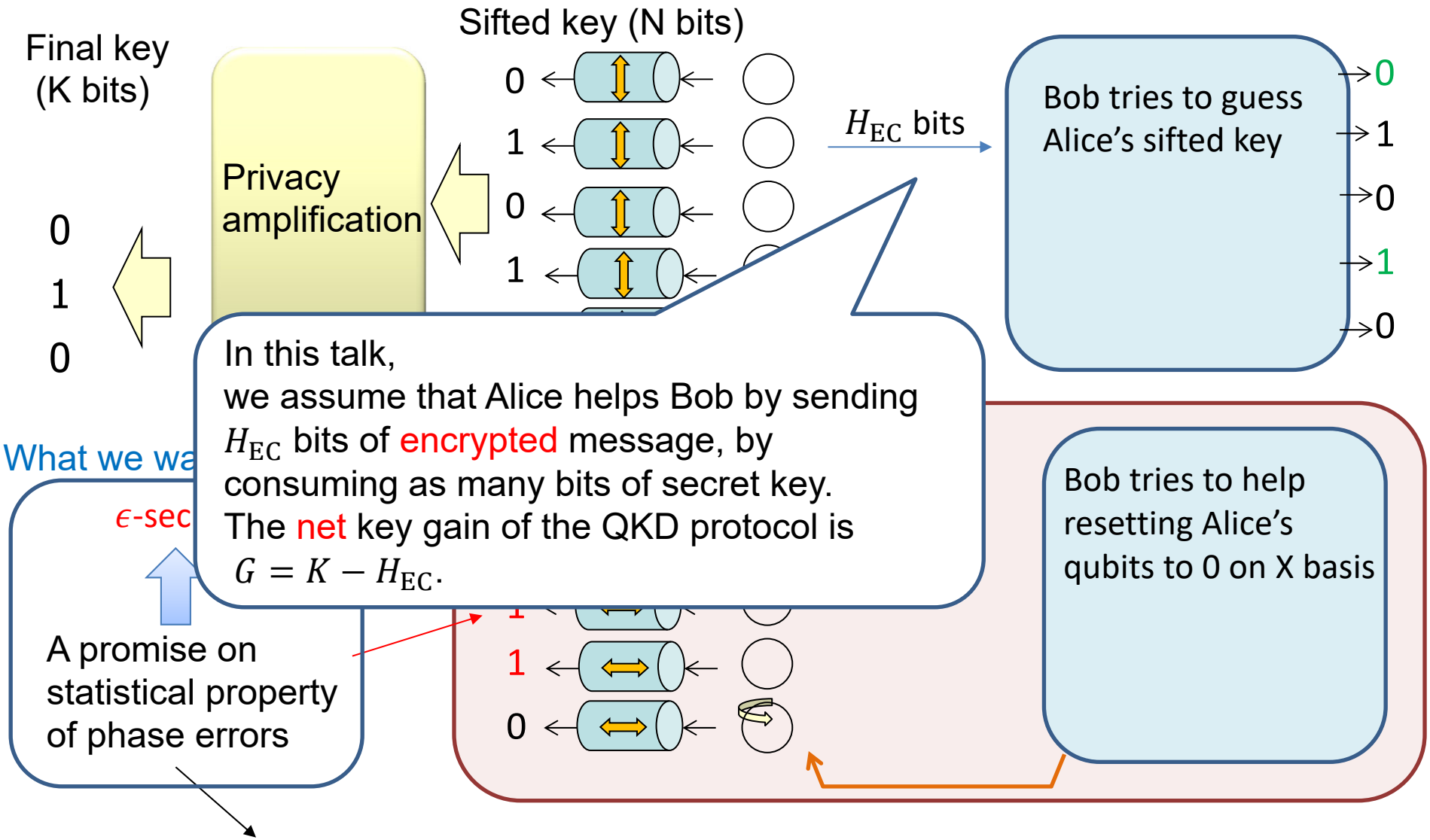


Realistic cases



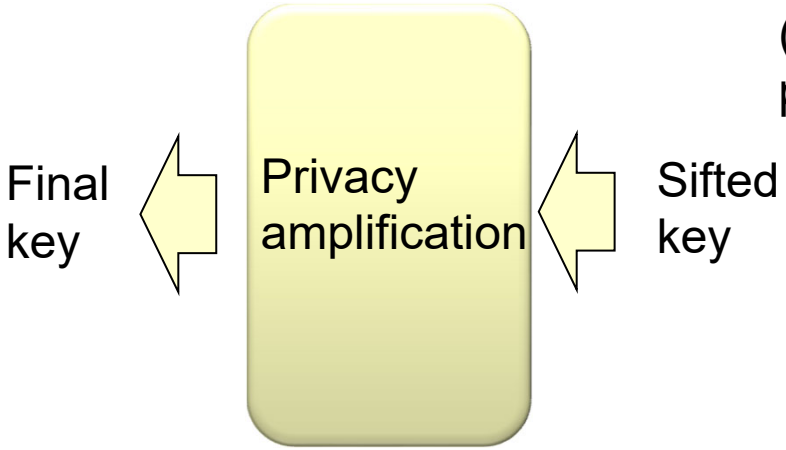
e.g. The number of phase errors $\leq Ne_{\mathrm{ph}}$
except a small probability δ_1

Realistic cases



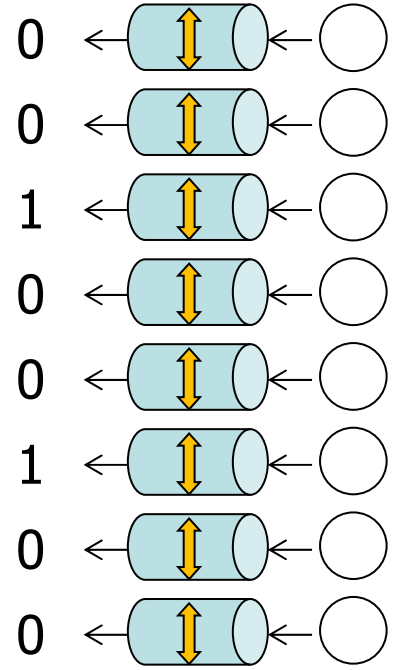
e.g. The number of phase errors $\leq Ne_{\mathrm{ph}}$
except a small probability δ_1

Privacy amplification



(Bob also applies the same procedure to his sifted key.)

Sifted key (N bits) N qubits



Final key (K bits)

0
1
0
1
0

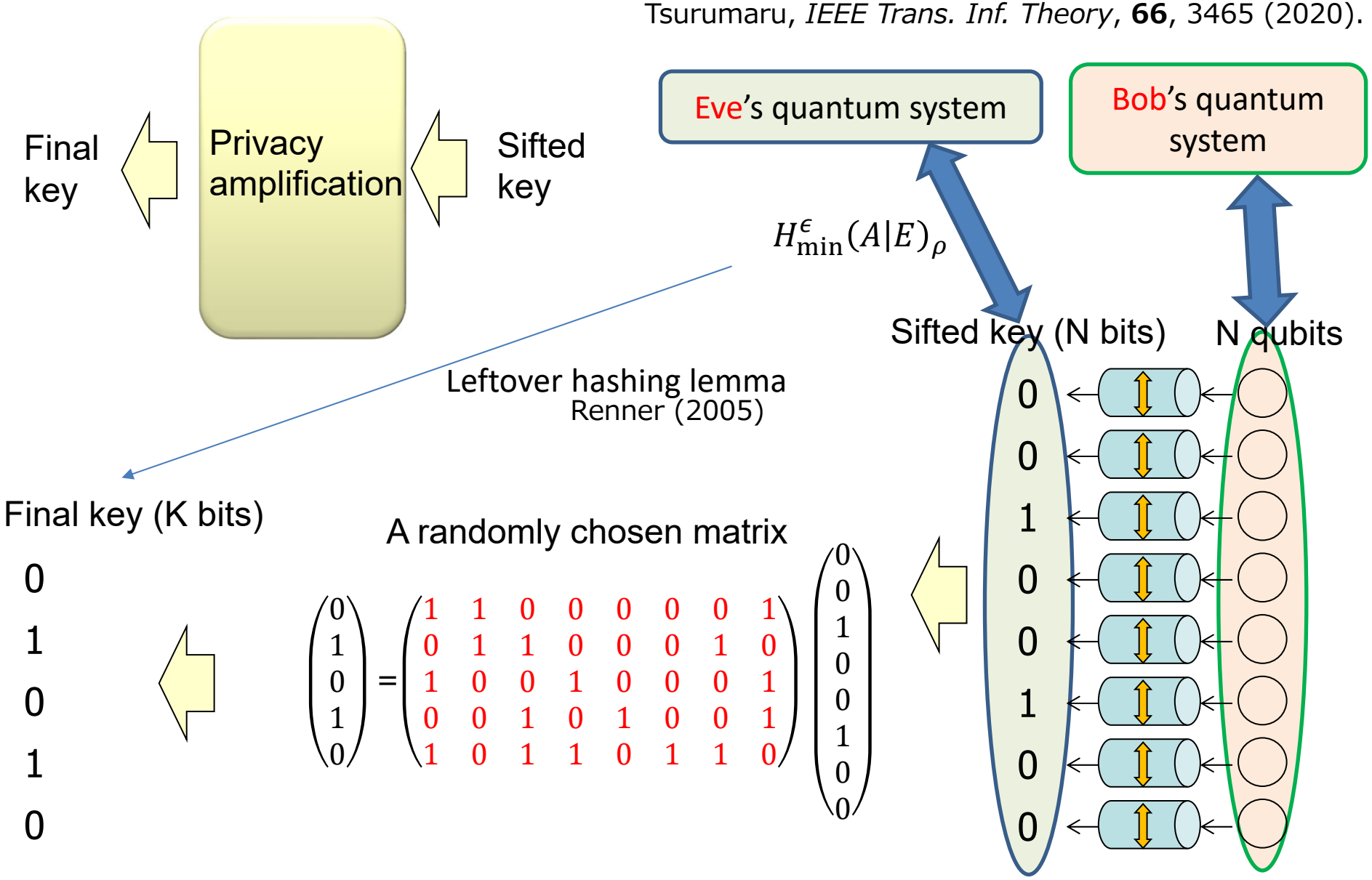
A randomly chosen matrix

$$\begin{pmatrix} 0 \\ 1 \\ 0 \\ 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 1 & 1 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 0 & 0 & 1 \\ 1 & 0 & 1 & 1 & 0 & 1 & 1 & 0 \end{pmatrix} \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \\ 0 \\ 1 \\ 0 \\ 0 \end{pmatrix}$$

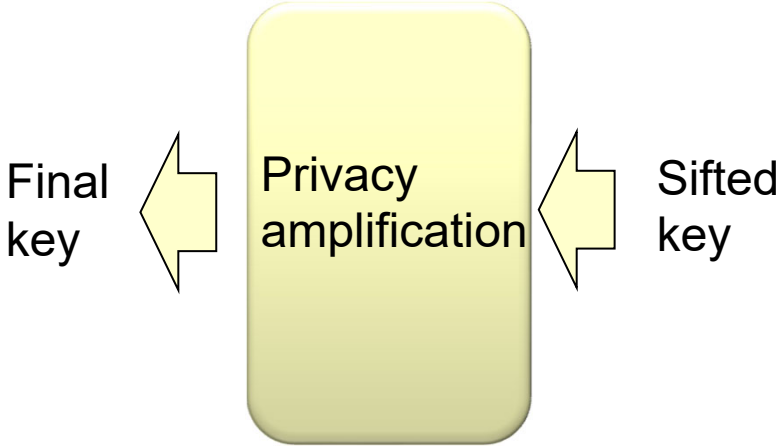
Approach with leftover hashing lemma

Relations between the two approaches

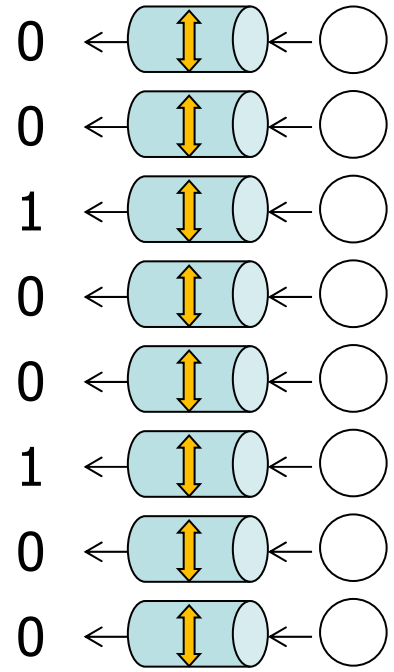
Tsurumaru, *IEEE Trans. Inf. Theory*, **66**, 3465 (2020).



Privacy amplification



Sifted key (N bits) N qubits



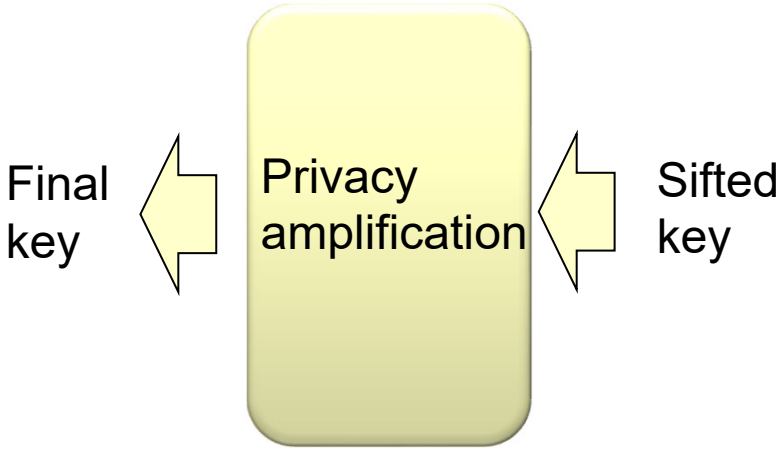
Final key (K bits)

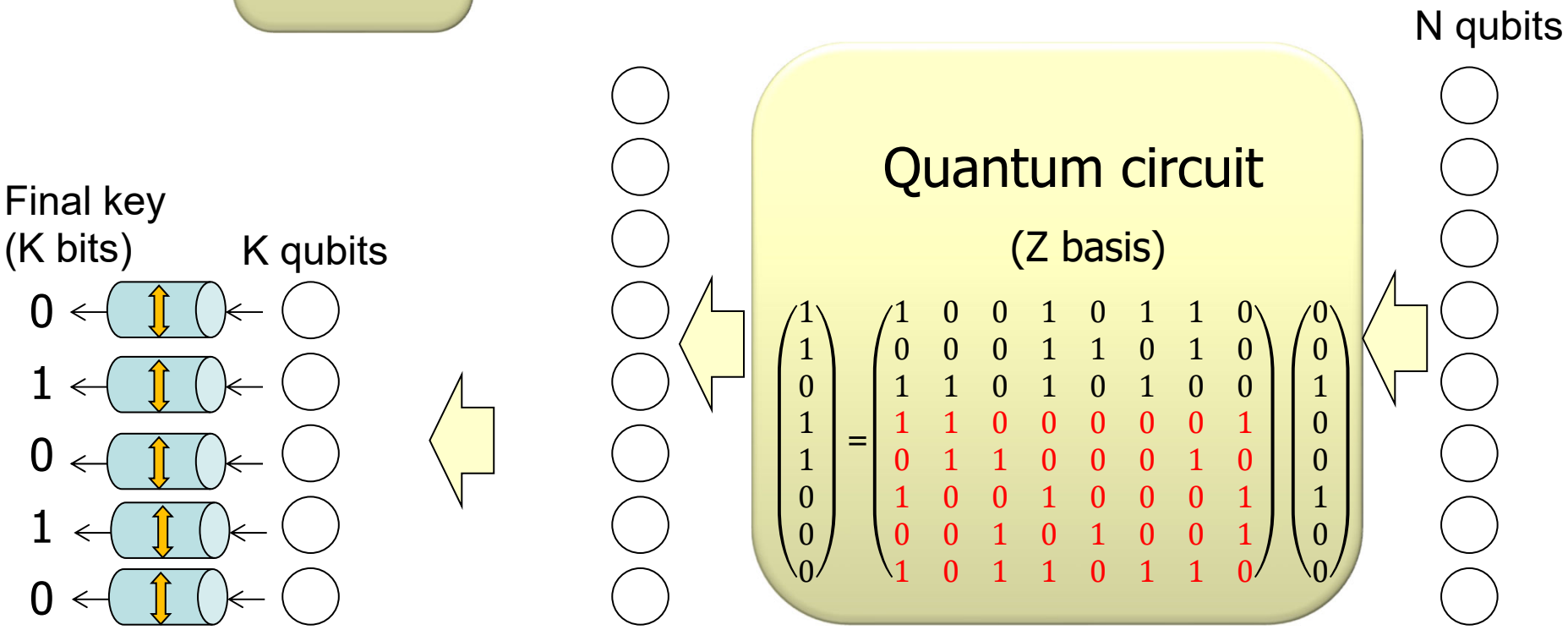
0
1
0
1
0

A randomly chosen matrix

$$\begin{pmatrix} 0 \\ 1 \\ 0 \\ 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 1 & 1 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 0 & 0 & 1 \\ 1 & 0 & 1 & 1 & 0 & 1 & 1 & 0 \end{pmatrix} \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \\ 0 \\ 1 \\ 0 \\ 0 \end{pmatrix}$$

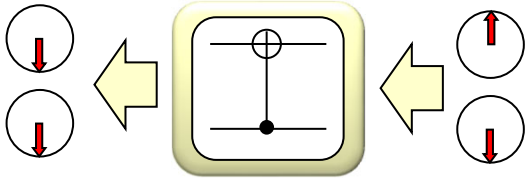
Privacy amplification





Example: a controlled-NOT gate

on Z basis



$$\begin{pmatrix}1\\1\end{pmatrix}=\begin{pmatrix}1 & 1\\0 & 1\end{pmatrix}\begin{pmatrix}0\\1\end{pmatrix}$$

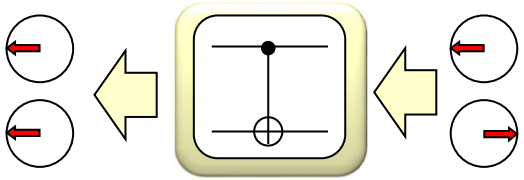
Matrix C

The same quantum circuit

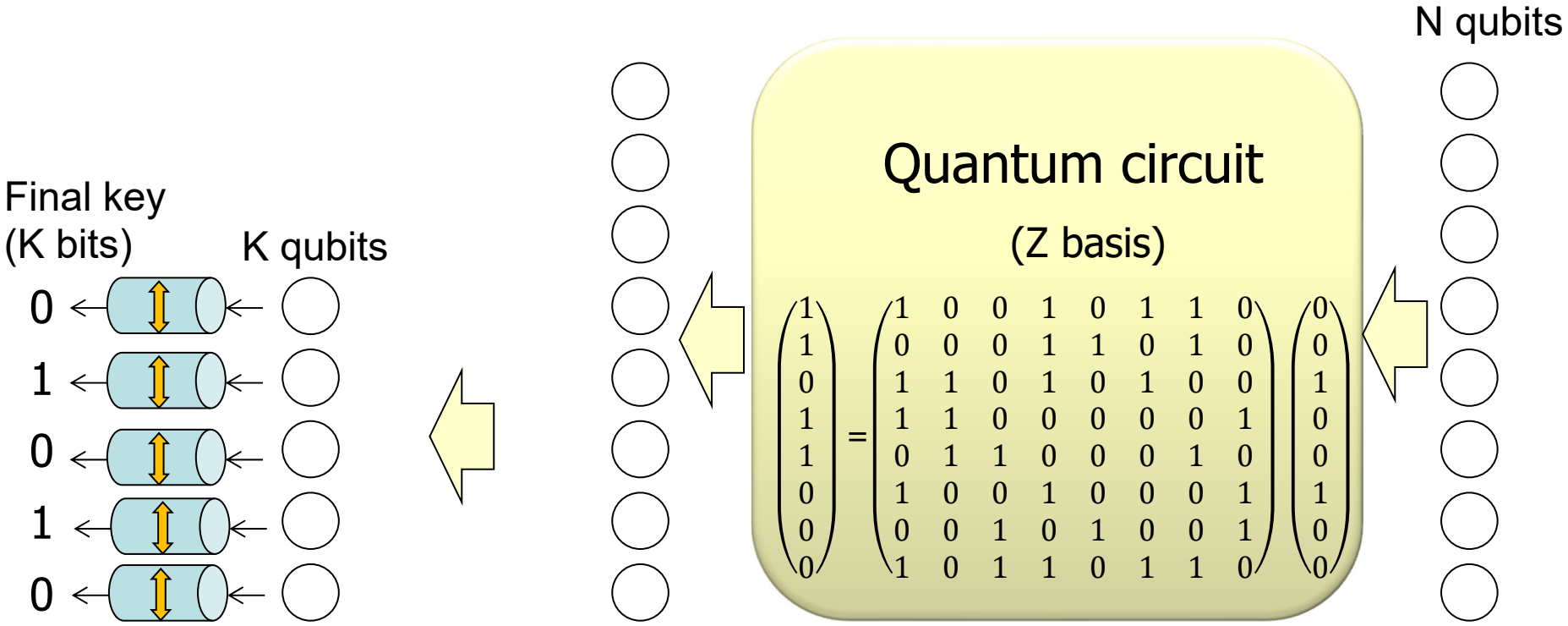
Matrix $(C^{-1})^{\mathrm{T}}$

$$\begin{pmatrix}1\\1\end{pmatrix}=\begin{pmatrix}1 & 0\\1 & 1\end{pmatrix}\begin{pmatrix}1\\0\end{pmatrix}$$

on X basis



Privacy amplification



Privacy amplification

On Z basis:

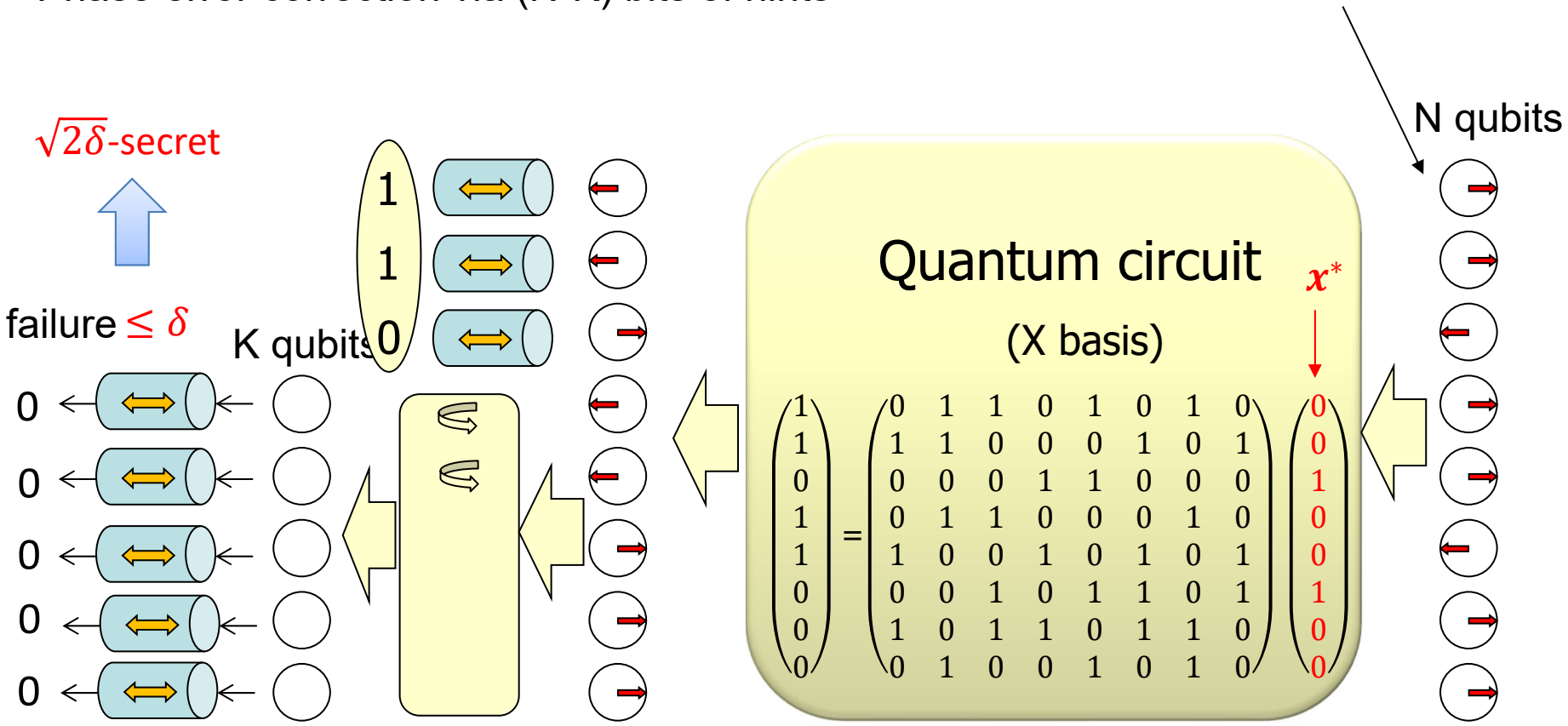
Privacy amplification to K bits

On X basis:

Phase error correction via (N-K) bits of hints

A promise on statistical property of phase error patterns $\boldsymbol{x}^*$

e.g. The number of phase errors $\leq Ne_{\mathrm{ph}}$ except a small probability δ_1



Amount of privacy amplification (Rough)

Phase error correction will succeed if

$$H_{\mathrm{ph}} \leq N - K$$

Secure final key length

$$K \cong N - H_{\mathrm{ph}}$$

Every bit halves the number of candidates.

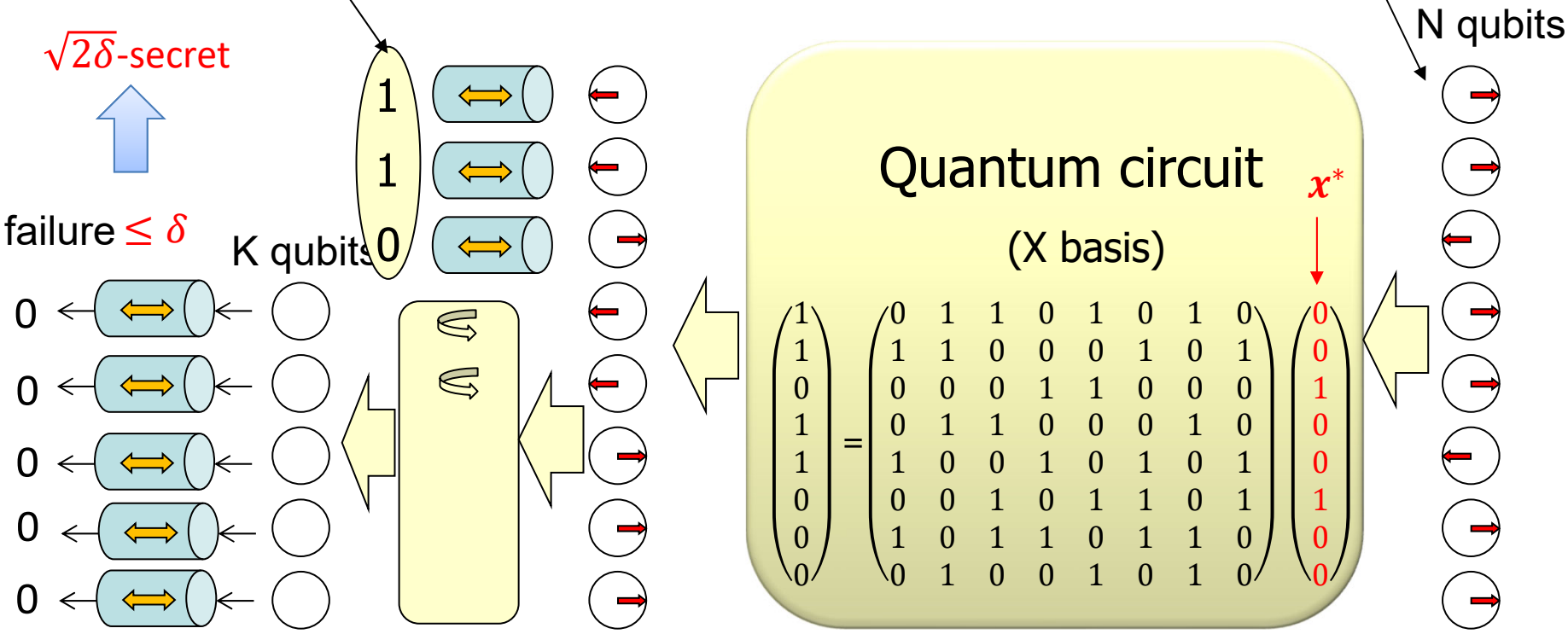
Number of possible phase error patterns $\leq 2^{H_{\mathrm{ph}}}$

(N-bit string $\boldsymbol{x}^*$)

e.g. The number of phase errors $\leq Ne_{\mathrm{ph}}$

$$H_{\mathrm{ph}} = Nh(e_{\mathrm{ph}})$$

$$h(x) \coloneqq -x\log_2 x - (1-x)\log(1-x)$$



Amount of privacy amplification (Strict)

Choose the final key length K as

$$K = N - H_{\mathrm{ph}} - s$$

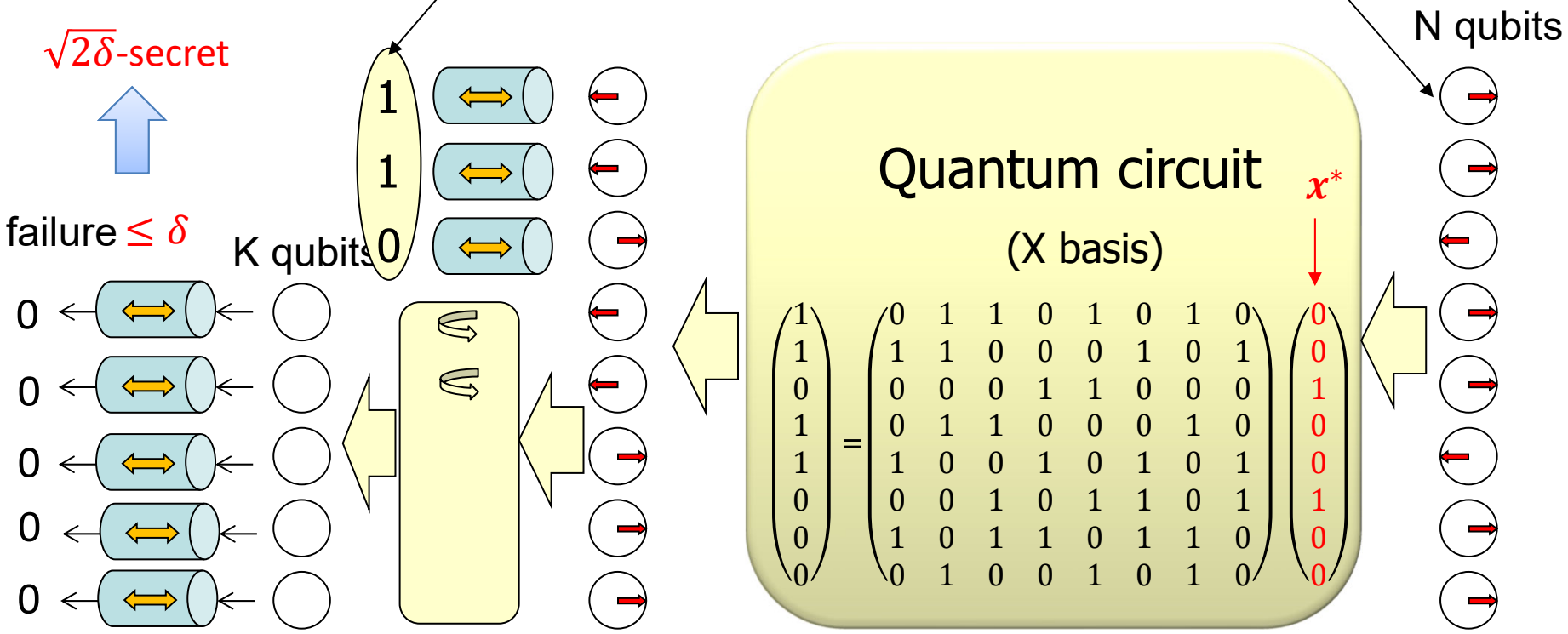
$$\text{failure} \le \delta = 2^{-(N-K)}|T| + \delta_1 \le 2^{-s} + \delta_1$$

One can choose a candidate set T of probable phase error patterns such that

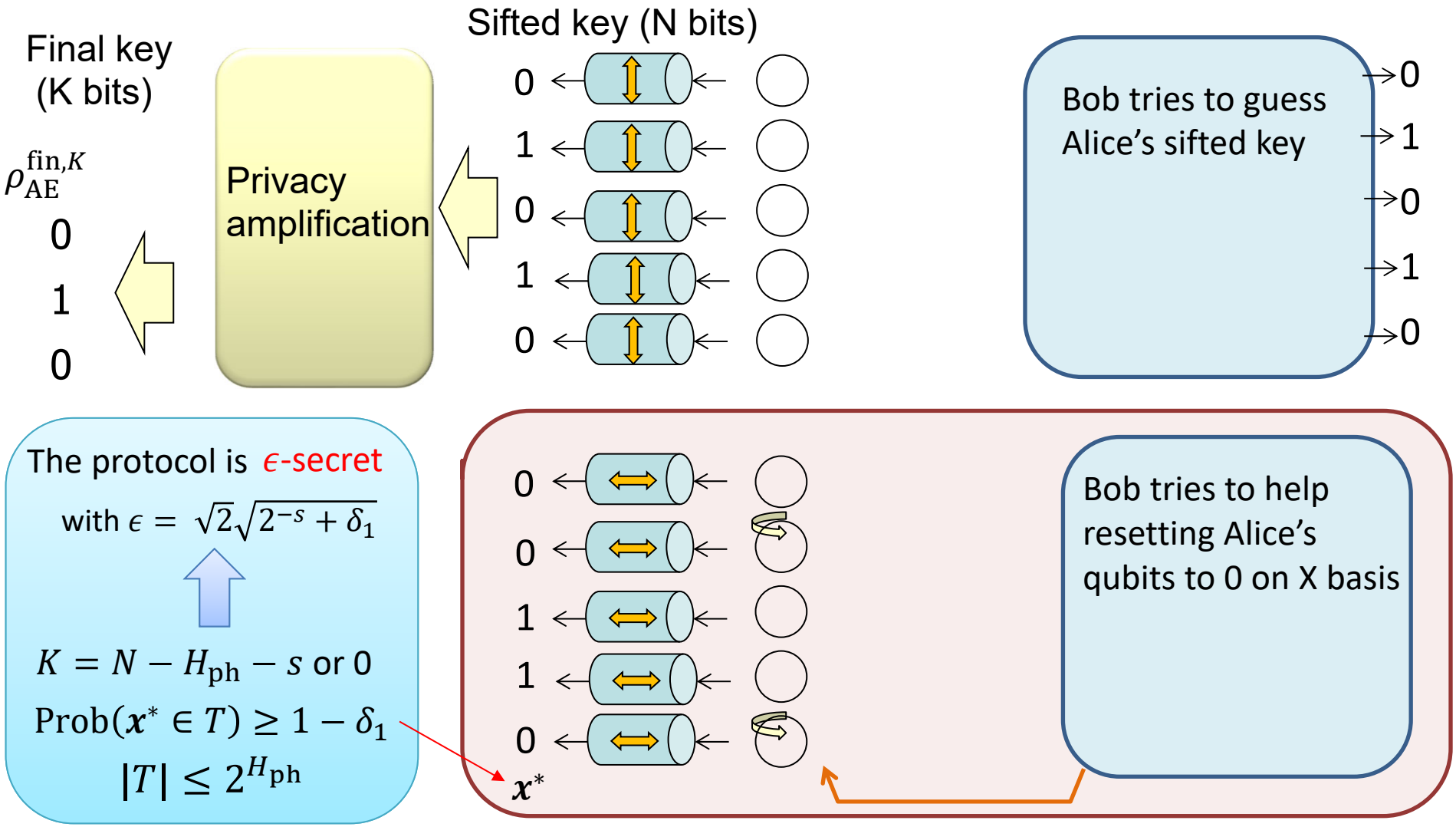
$$\mathrm{Prob}(\boldsymbol{x}^* \in T) \ge 1 - \delta_1$$

$$|T| \le 2^{H_{\mathrm{ph}}}$$

Every wrong candidate in T is eliminated except probability $2^{-(N-K)}$

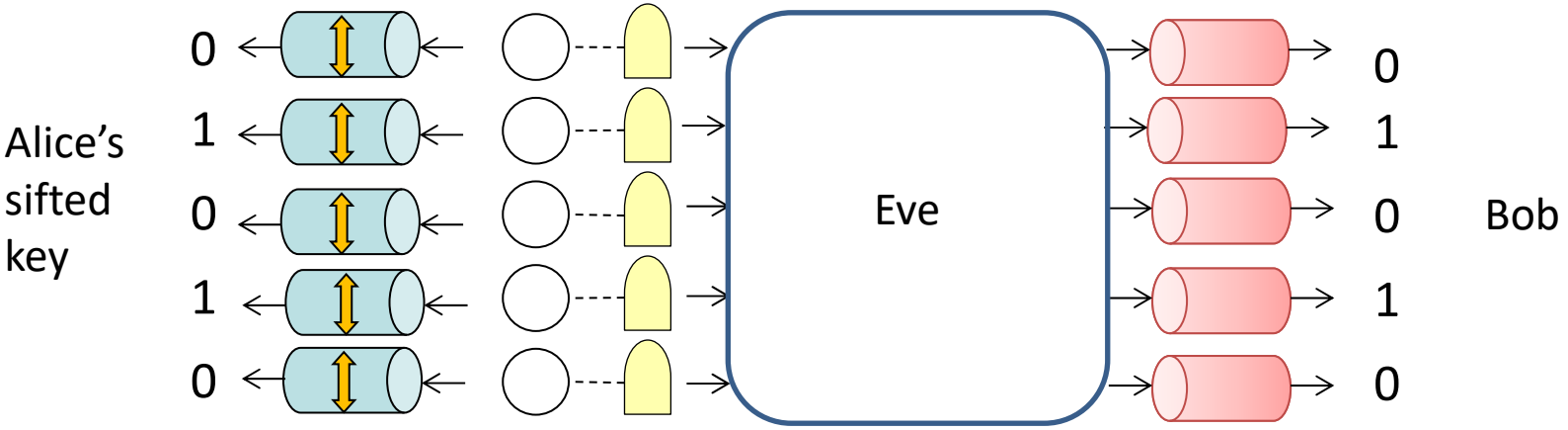


Finite-size security

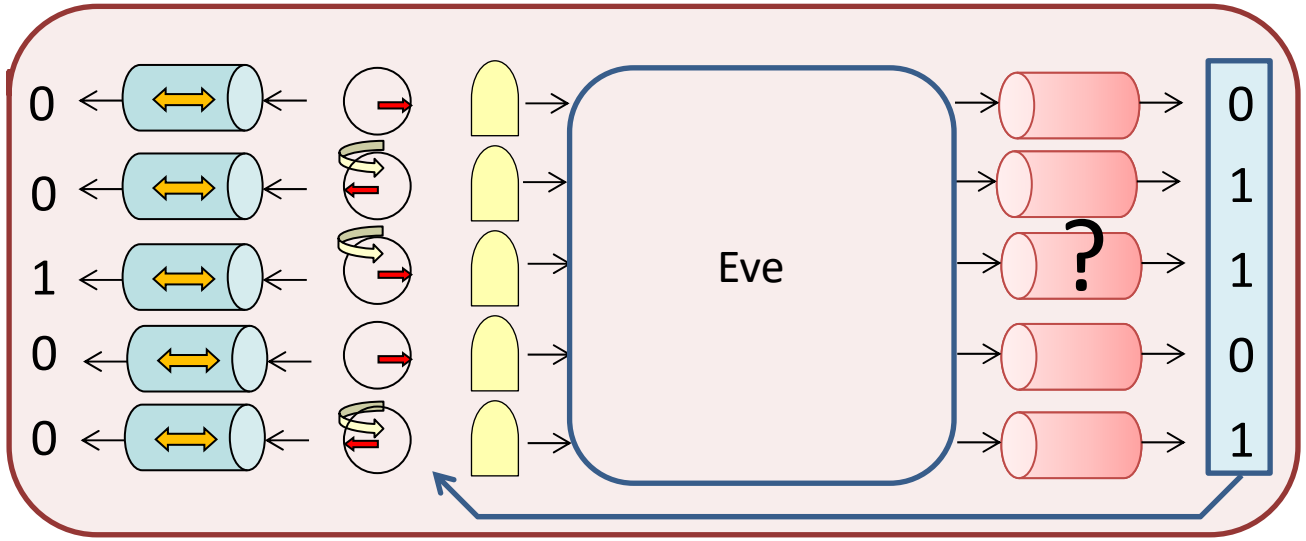


Recipe

1. Rewrite the protocol such that Alice's sifted key is the Z values of qubits.



2. Find what Bob could have done to help reducing phase errors.
(It must be compatible to Bob's announcement)



3. Compute a bound on the number of phase error patterns.

Remarks

'Phase error probability' or 'Phase error rate' e_{ph} in the asymptotic limit

Number of phase errors$\leq N(e_{\mathrm{ph}} + \delta_2^{(N)})$
except probability $\delta_1^{(N)}$

$$\delta_1^{(N)}, \delta_2^{(N)} \to 0 \quad \text{for } N \to \infty$$

$$H_{\mathrm{ph}} = Nh(e_{\mathrm{ph}} + \delta_2^{(N)})$$

Asymptotic efficiency of privacy amplification

$$\frac{K}{N} = 1 - h\left(e_{\mathrm{ph}} + \delta_2^{(N)}\right) - \frac{s}{N} \to 1 - h(e_{\mathrm{ph}})$$

The protocol is ϵ-secret with $\epsilon = \sqrt{2}\sqrt{2^{-s} + \delta_1}$

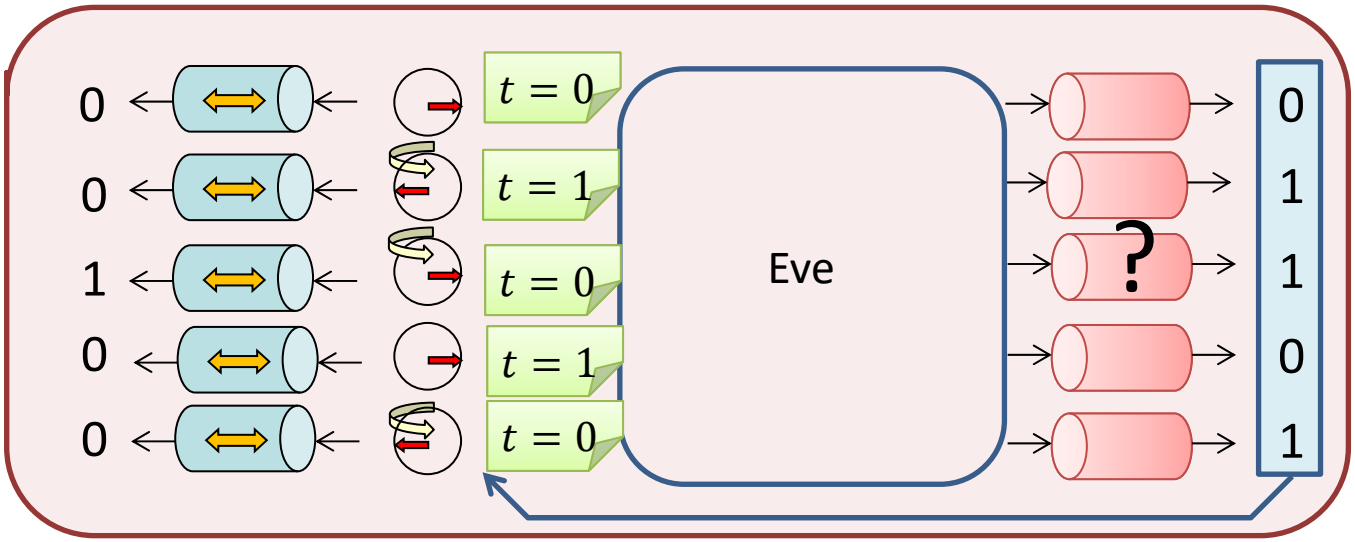
$$K = N - H_{\mathrm{ph}} - s \text{ or } 0$$

$$\mathrm{Prob}(\boldsymbol{x}^* \in T) \geq 1 - \delta_1$$

$$|T| \leq 2^{H_{\mathrm{ph}}}$$

Remarks

Tagging



Sifted key bits are tagged and classified: $N = \sum_t N^{(t)}$ $\quad \frac{N^{(t)}}{N} \to Q^{(t)}$

Phase error probability $e_{\mathrm{ph}}^{(t)}$ depending on the tag value t

Number of phase error patterns: $\sim \prod_t 2\text{^}[N^{(t)} h\left(e_{\mathrm{ph}}^{(t)}\right)]$

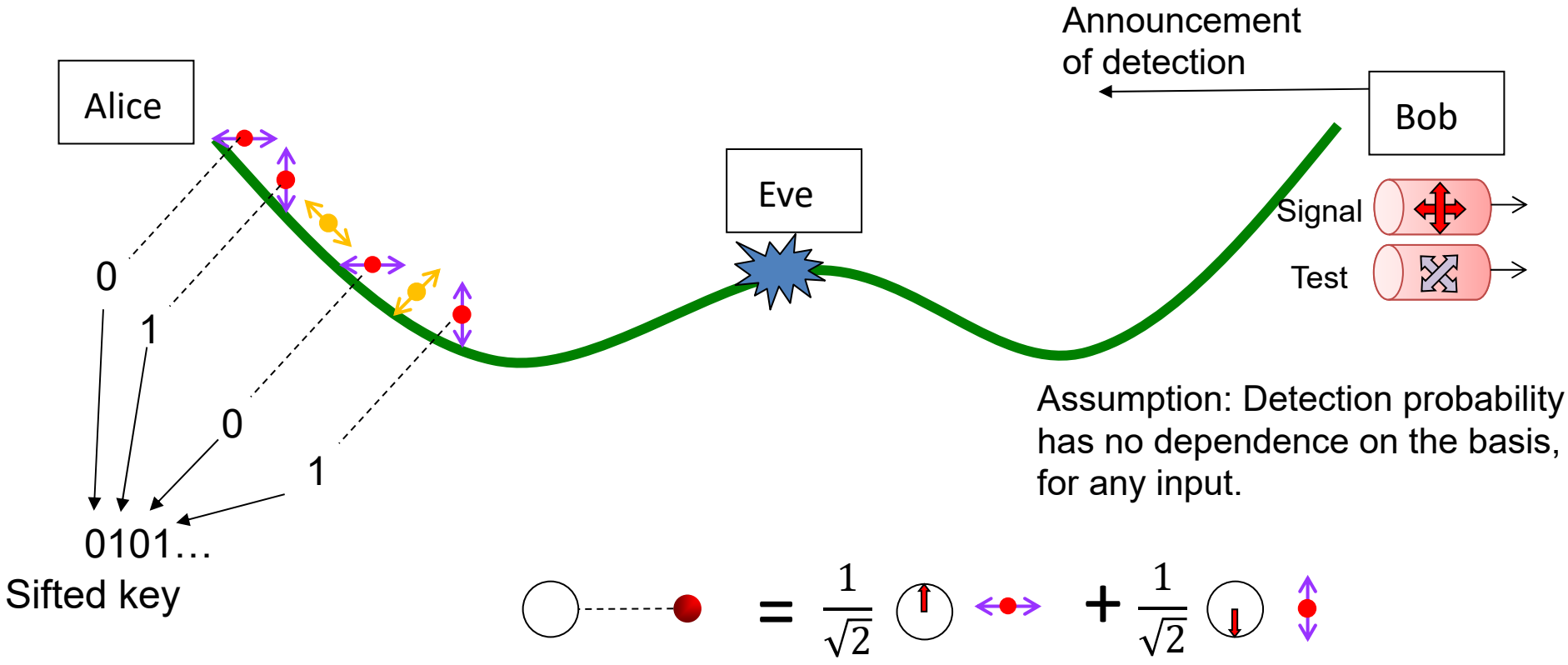
$$H_{\mathrm{ph}} \sim \sum_t N^{(t)} h\left(e_{\mathrm{ph}}^{(t)}\right)$$

$$\frac{K}{N} \to 1 - \sum_t Q^{(t)} h\left(e_{\mathrm{ph}}^{(t)}\right)$$

Gottesman, Lo, Lutkenhaus, Preskill, Quant. Inf. Comput. **5**, 325 (2004).

PART II: Protocols

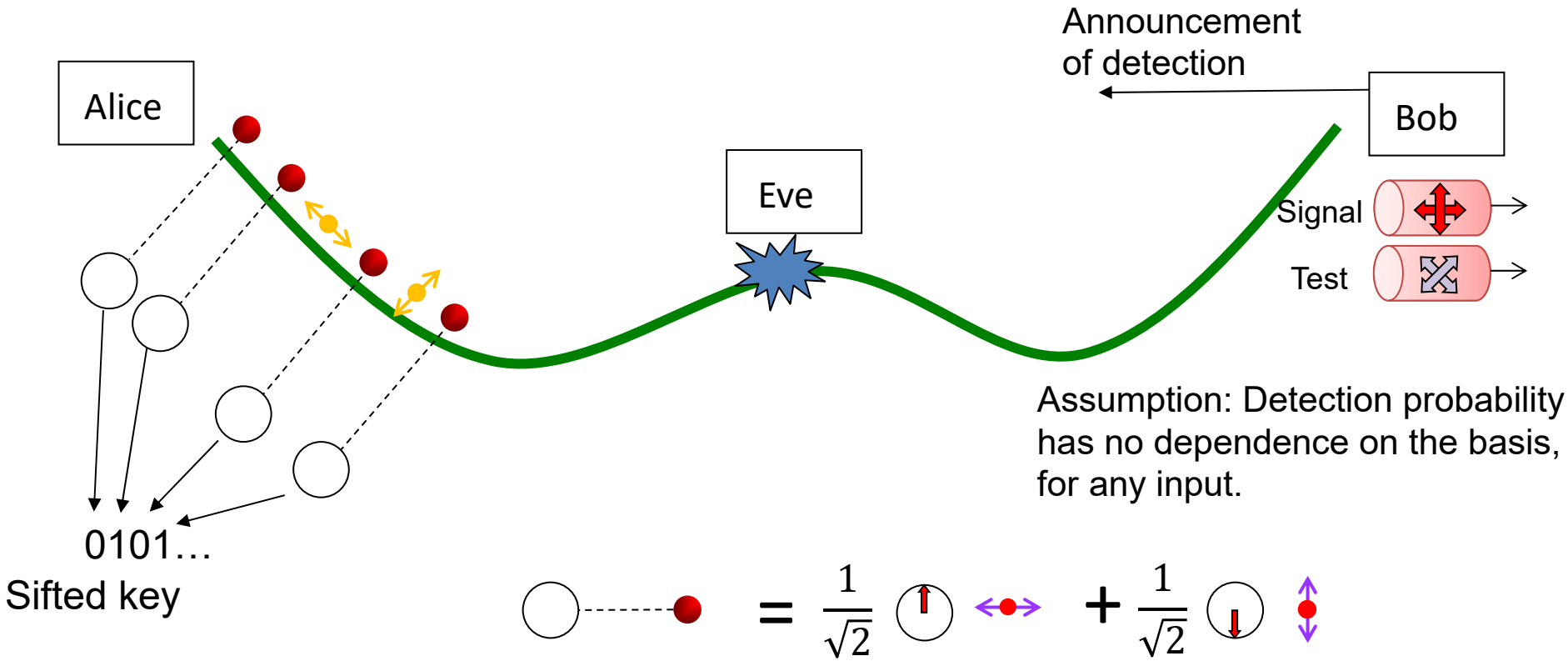
Ideal BB84 protocol



$$= \frac{1}{\sqrt{2}} + \frac{1}{\sqrt{2}}$$

	Signal	Test
0		
1		

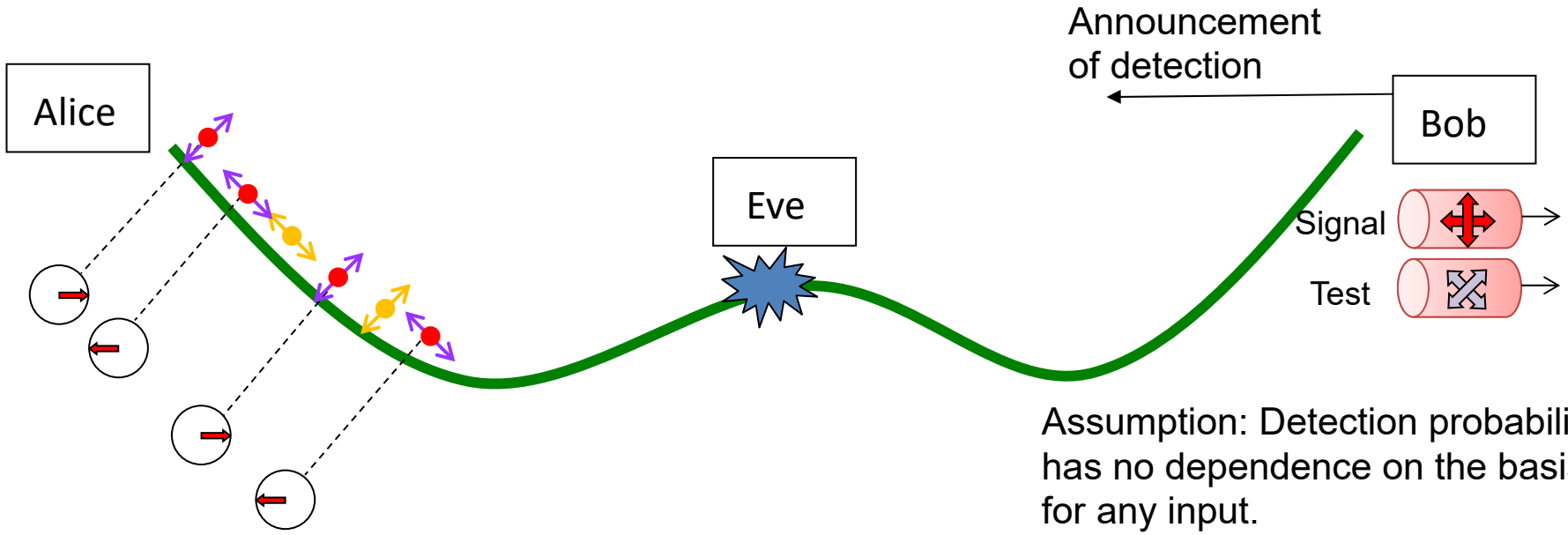
Ideal BB84 protocol



$$= \frac{1}{\sqrt{2}} + \frac{1}{\sqrt{2}}$$

	Signal	Test
0	↔	⤢
1	↕	⤡

Ideal BB84 protocol



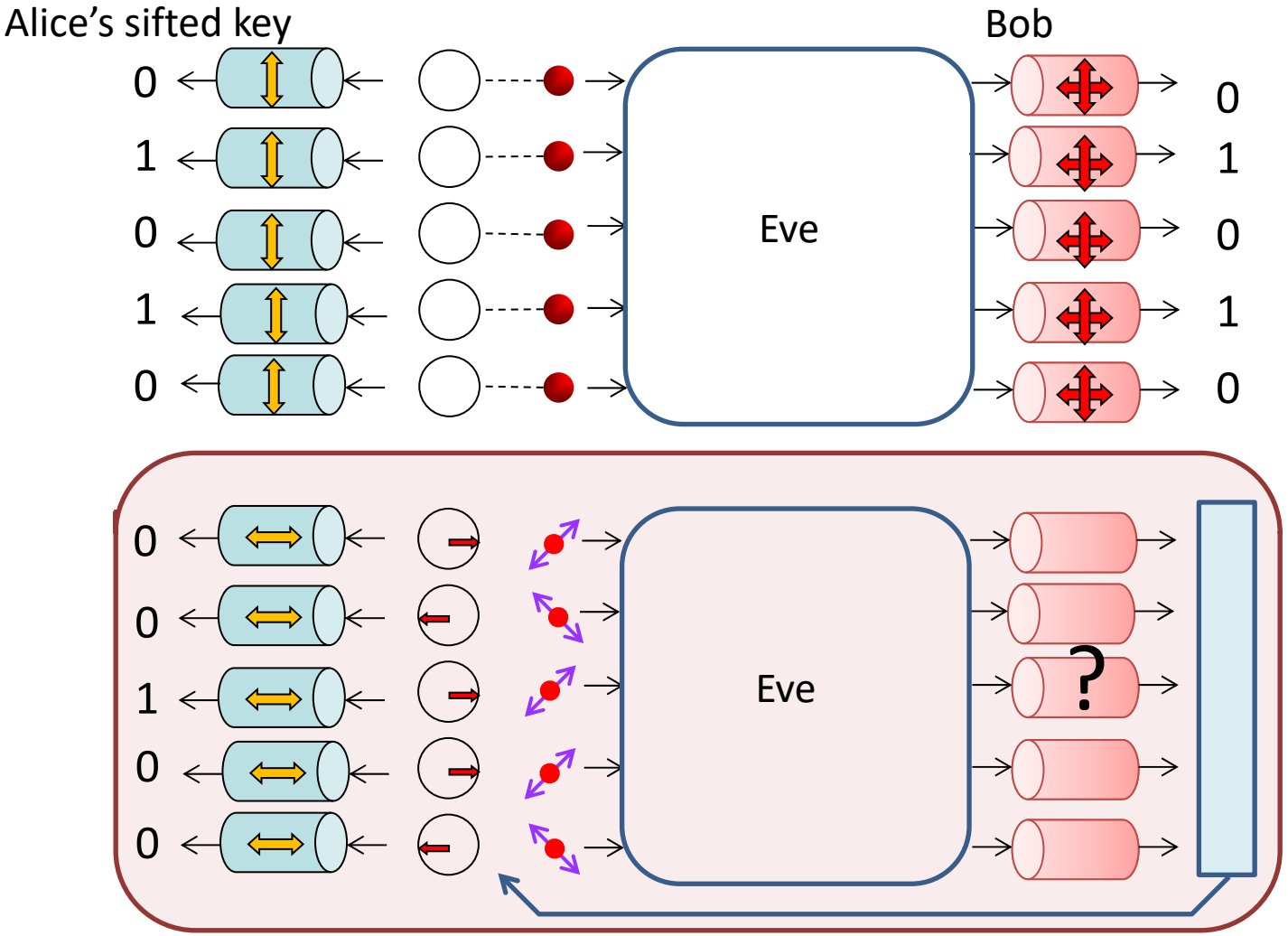
Assumption: Detection probability has no dependence on the basis, for any input.

$$= \frac{1}{\sqrt{2}} + \frac{1}{\sqrt{2}}$$

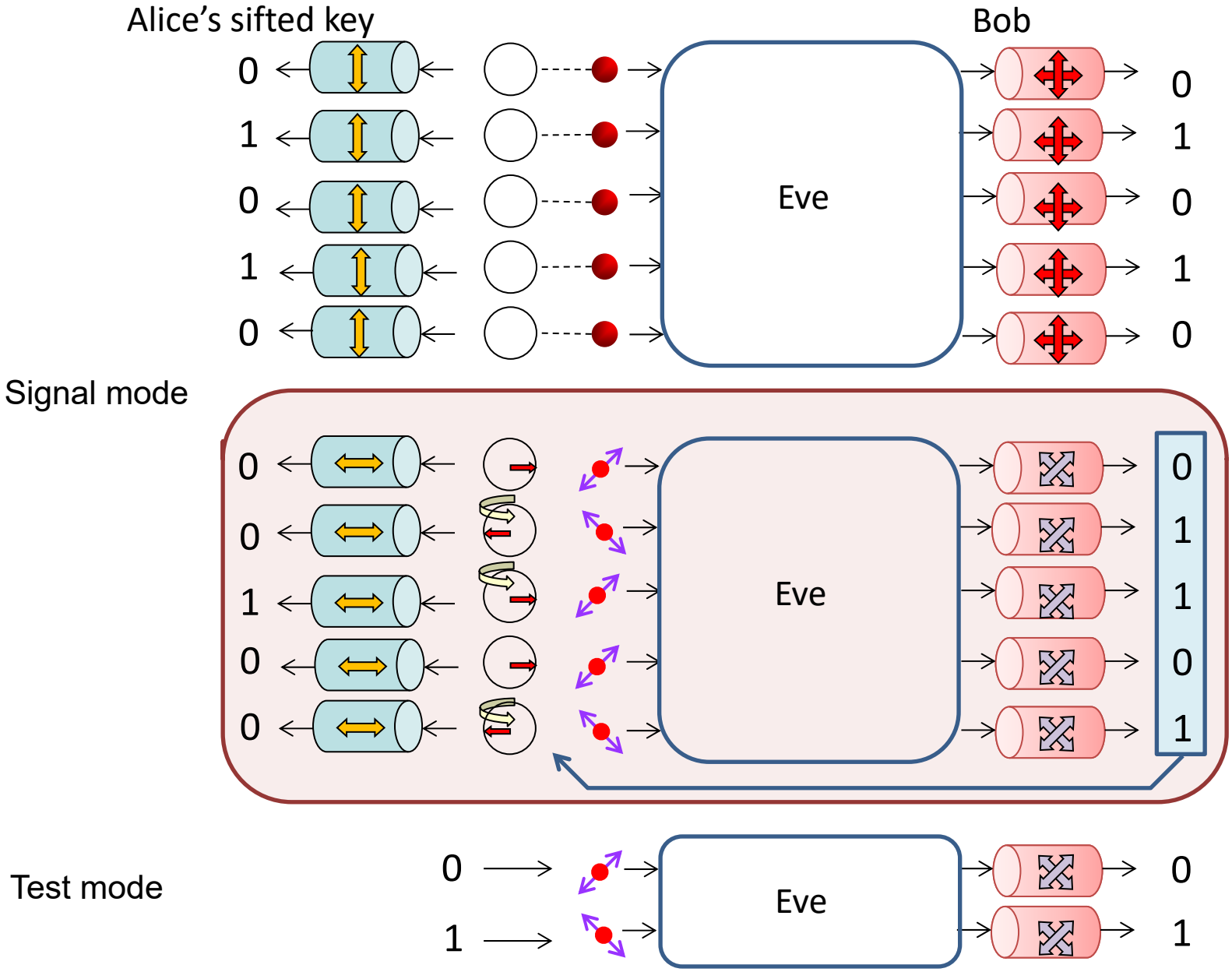
$$= \frac{1}{\sqrt{2}} + \frac{1}{\sqrt{2}}$$

	Signal	Test
0		
1		

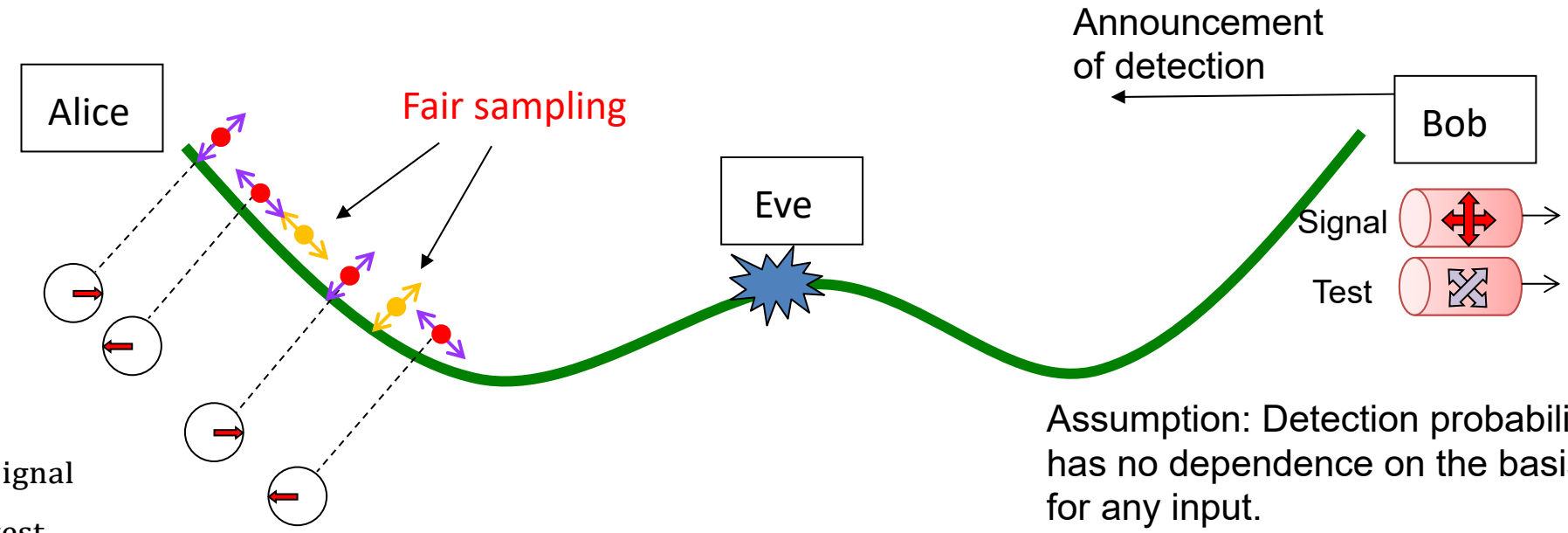
Ideal BB84 protocol



Ideal BB84 protocol



Ideal BB84 protocol



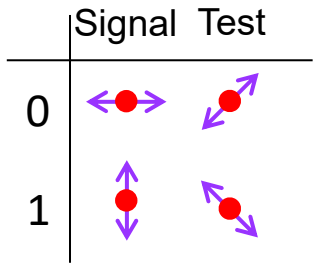
Assumption: Detection probability has no dependence on the basis, for any input.

P_{signal}

P_{test}

$$P = \frac{P_{\text{test}}}{P_{\text{signal}} + P_{\text{test}}}$$

Errors found in the test mode are fair sampling of phase errors



Asymptotic key length: $K \sim N(1 - h(e_{\text{test}}))$

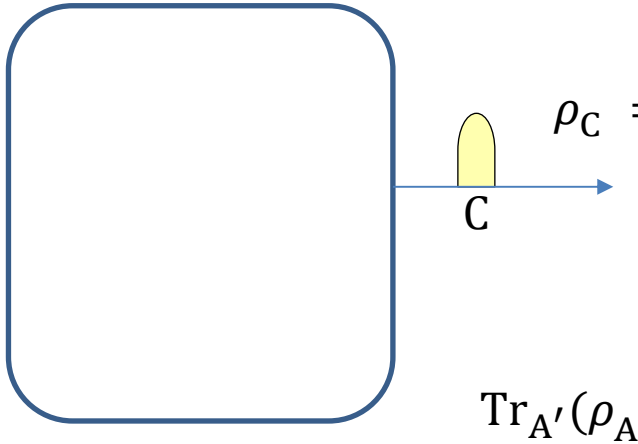
Finite-size: classical sampling theory is enough.

Simple random sampling	A fixed number of samples drawn	Hypergeometric distribution
Bernoulli sampling	Samples drawn with a fixed probability P	Binomial distribution

Kawakami, Sasaki, MK, *Phys. Rev. A*, **96**, 012305 (2017).

BB84 protocol with phase-randomized laser pulses

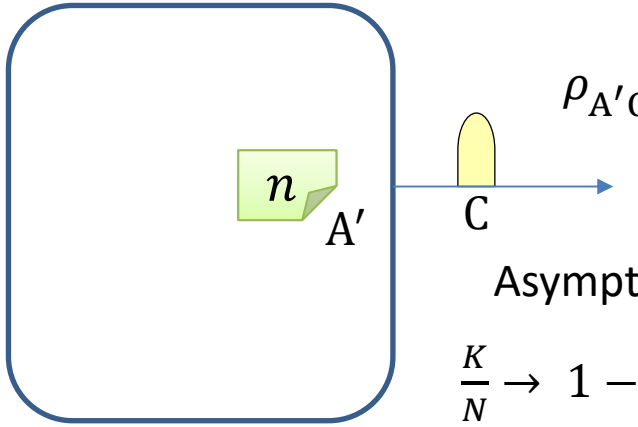
Alice emits a phase-randomized pulse in a mode C



$$\rho_{\mathrm{C}} = \sum_{n=0}^{\infty} p(n)|n\rangle\langle n|_{\mathrm{C}}$$

n: number of photons

$$\mathrm{Tr}_{\mathrm{A}'}(\rho_{\mathrm{A}'\mathrm{C}}) = \rho_{\mathrm{C}}$$



$$\rho_{\mathrm{A}'\mathrm{C}} = \sum_{n=0}^{\infty} p(n)|n\rangle\langle n|_{\mathrm{A}'}|n\rangle\langle n|_{\mathrm{C}}$$

Asymptotic rate

$$\frac{K}{N} \to 1 - Q^{(n=0)} h\left(e_{\mathrm{ph}}^{(n=0)}\right) - Q^{(n=1)} h\left(e_{\mathrm{ph}}^{(n=1)}\right) - Q^{(n\geq 2)} h\left(e_{\mathrm{ph}}^{(n\geq 2)}\right)$$

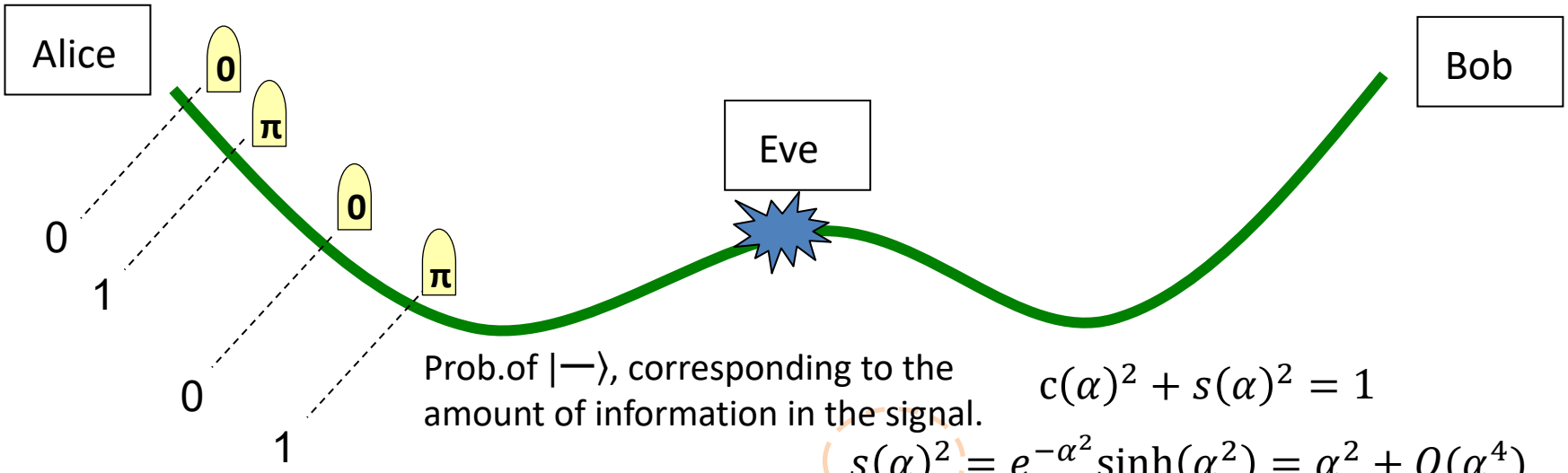
$$= 1 - Q^{(n=1)} h\left(e_{\mathrm{ph}}^{(n=1)}\right) - Q^{(n\geq 2)}$$

Tighter estimation of the parameters is done by decoy-state technique.

Lo, arXiv:quant-ph/0503004

Binary phase encoding

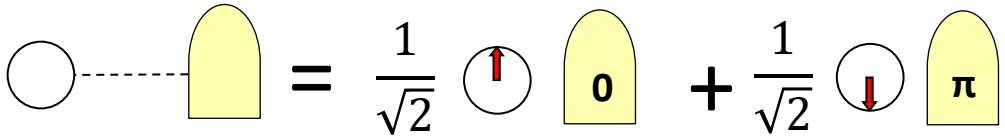
Used in many protocols: B92, DPS, RRPDS, a Twin-field(PM), a DM-CV, …



Prob.of |—⟩, corresponding to the amount of information in the signal.

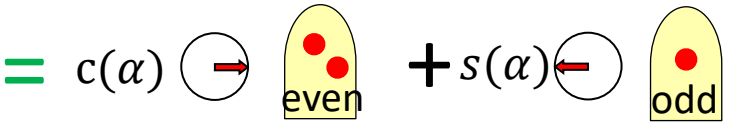
$$c(\alpha)^2 + s(\alpha)^2 = 1$$

$$s(\alpha)^2 = e^{-\alpha^2}\sinh(\alpha^2) = \alpha^2 + O(\alpha^4)$$



	Signal	
0	0	$\lvert +\alpha\rangle$
1	π	$\lvert -\alpha\rangle$

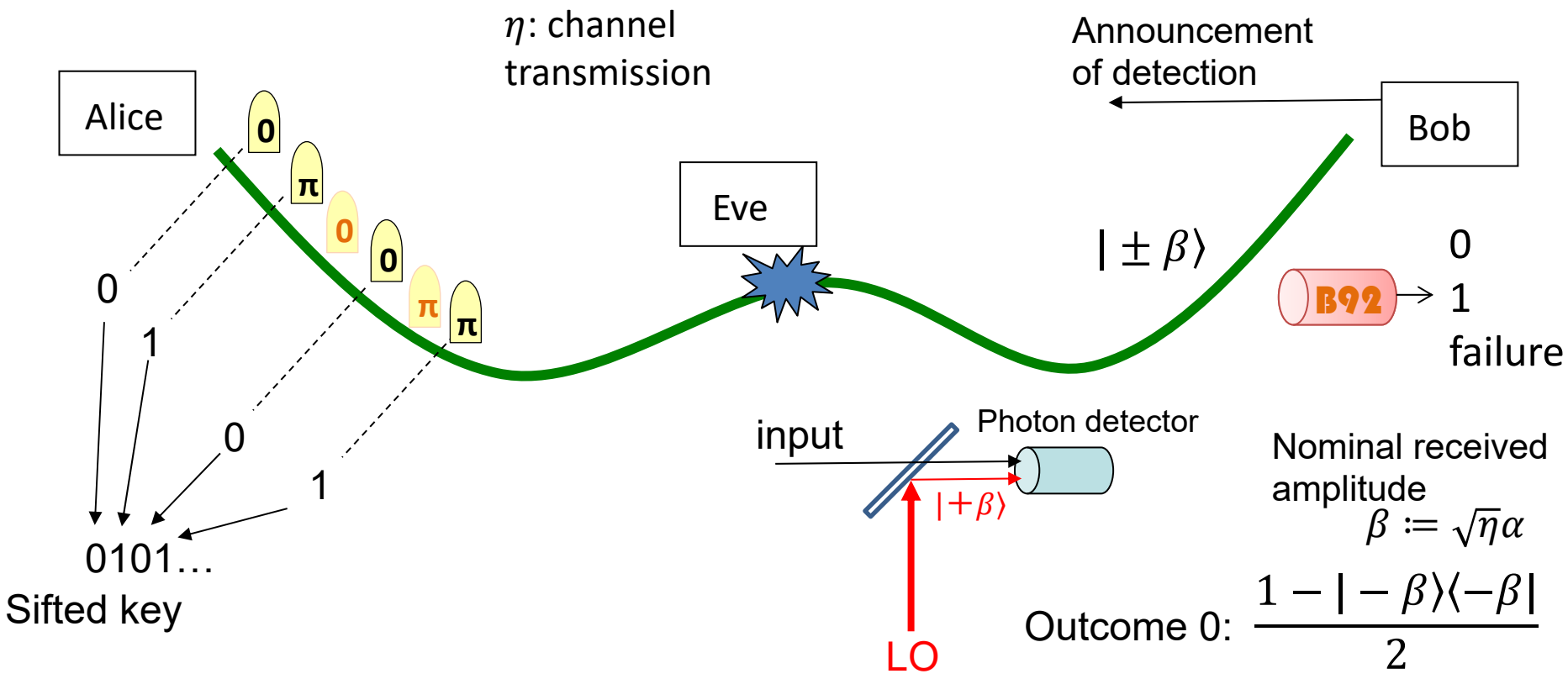
Coherent states



$|\alpha_{\mathrm{ev}}\rangle$ $|\alpha_{\mathrm{od}}\rangle$

Schrodinger cat states

B92 protocol



Nominal received amplitude

$$\beta := \sqrt{\eta}\alpha$$

Outcome 0: $\dfrac{1 - |-\beta\rangle\langle-\beta|}{2}$

Outcome 1: $\dfrac{1 - |+\beta\rangle\langle+\beta|}{2}$

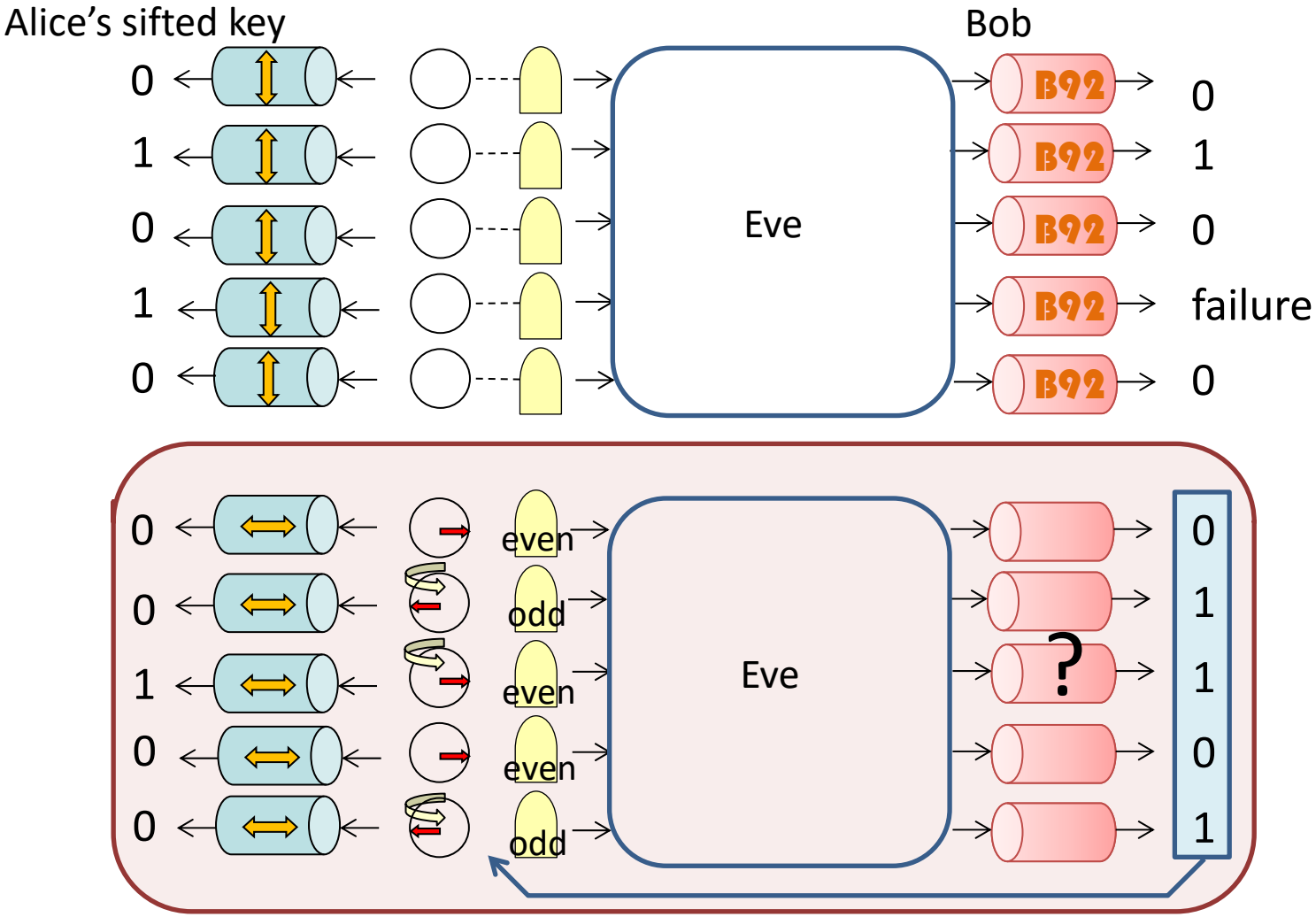
Outcome 'failure':

$$c(\beta)^2 |\beta_{\mathrm{ev}}\rangle\langle\beta_{\mathrm{ev}}| + s(\beta)^2 |\beta_{\mathrm{od}}\rangle\langle\beta_{\mathrm{od}}|$$

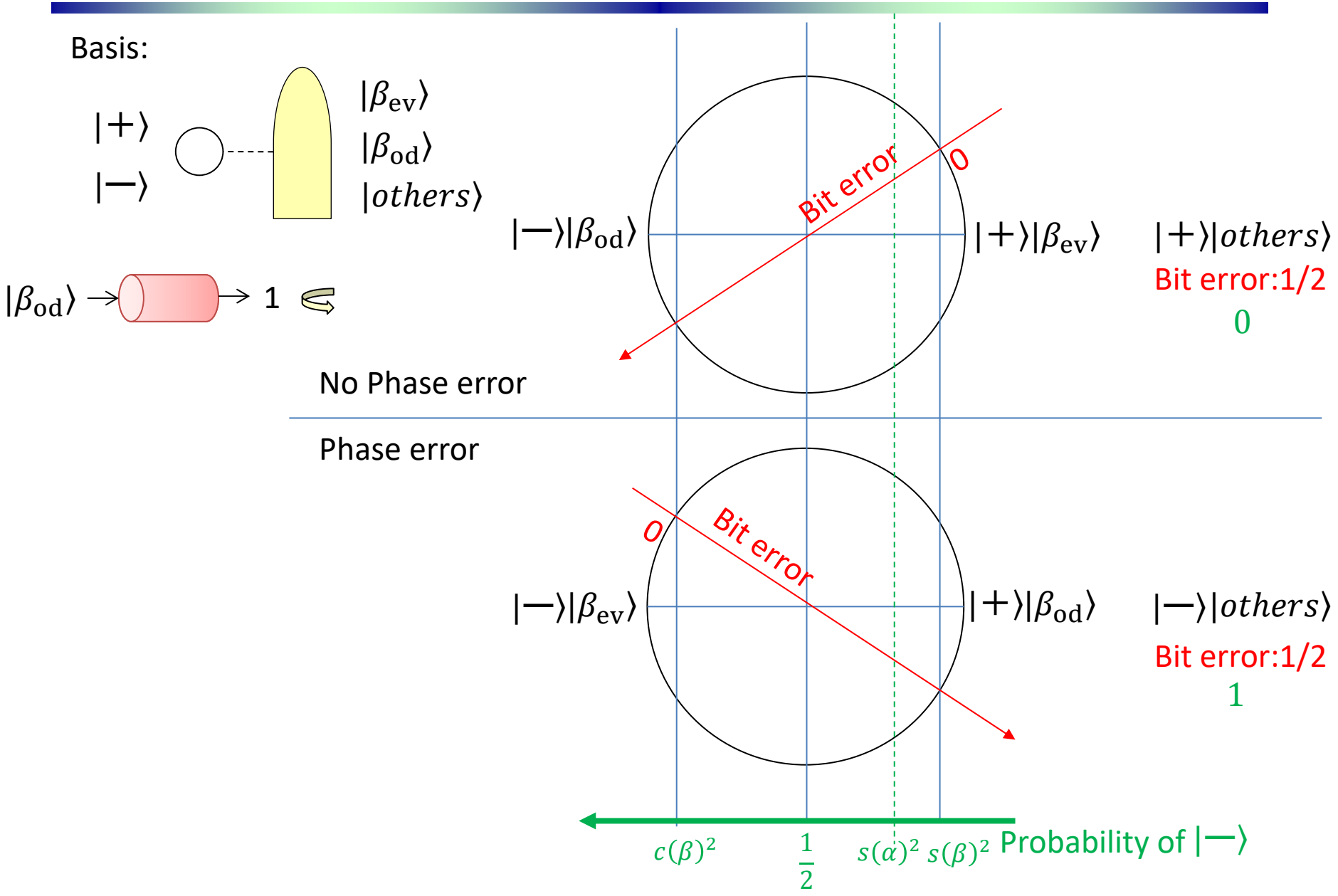
	Signal	Test	
0	0	0	$\|+\alpha\rangle$
1	π	π	$\|-\alpha\rangle$

Coherent states

B92 protocol



B92 protocol: Analysis of phase error probability



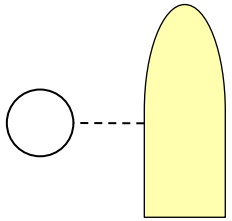
Tamaki, MK, Imoto, *Phys. Rev. Lett.*, **90**, 167904 (2003), MK, *Phys. Rev. Lett.*, **93**, 120501 (2004)

B92 protocol: Analysis of phase error probability

Basis:

$|+\rangle$

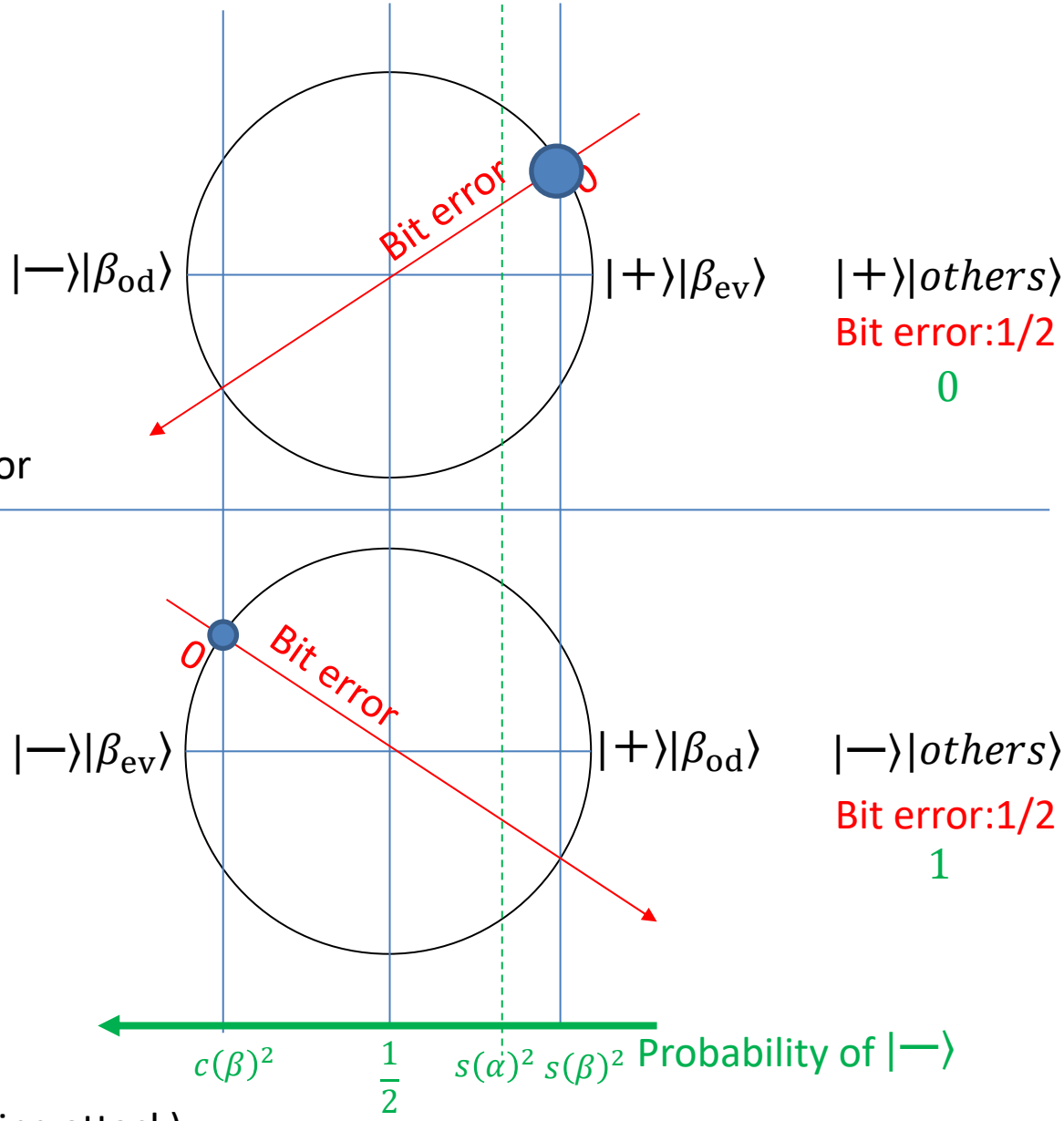
$|-\rangle$



$|\beta_{\mathrm{ev}}\rangle$

$|\beta_{\mathrm{od}}\rangle$

$|others\rangle$



If bit error prob. is zero ….

Only the two states are allowed.

The average must be the initial value $s(\alpha)^2$, since Eve cannot touch Alice's qubit.

Phase error probability is

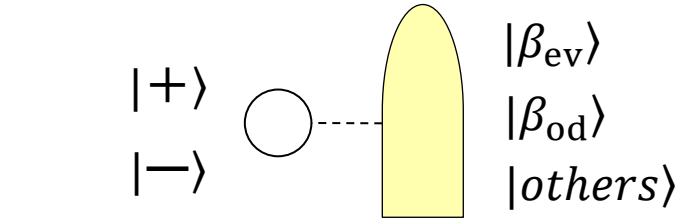
$$e_{\mathrm{ph}} = s\left(\sqrt{\alpha^2 - \beta^2}\right)^2$$

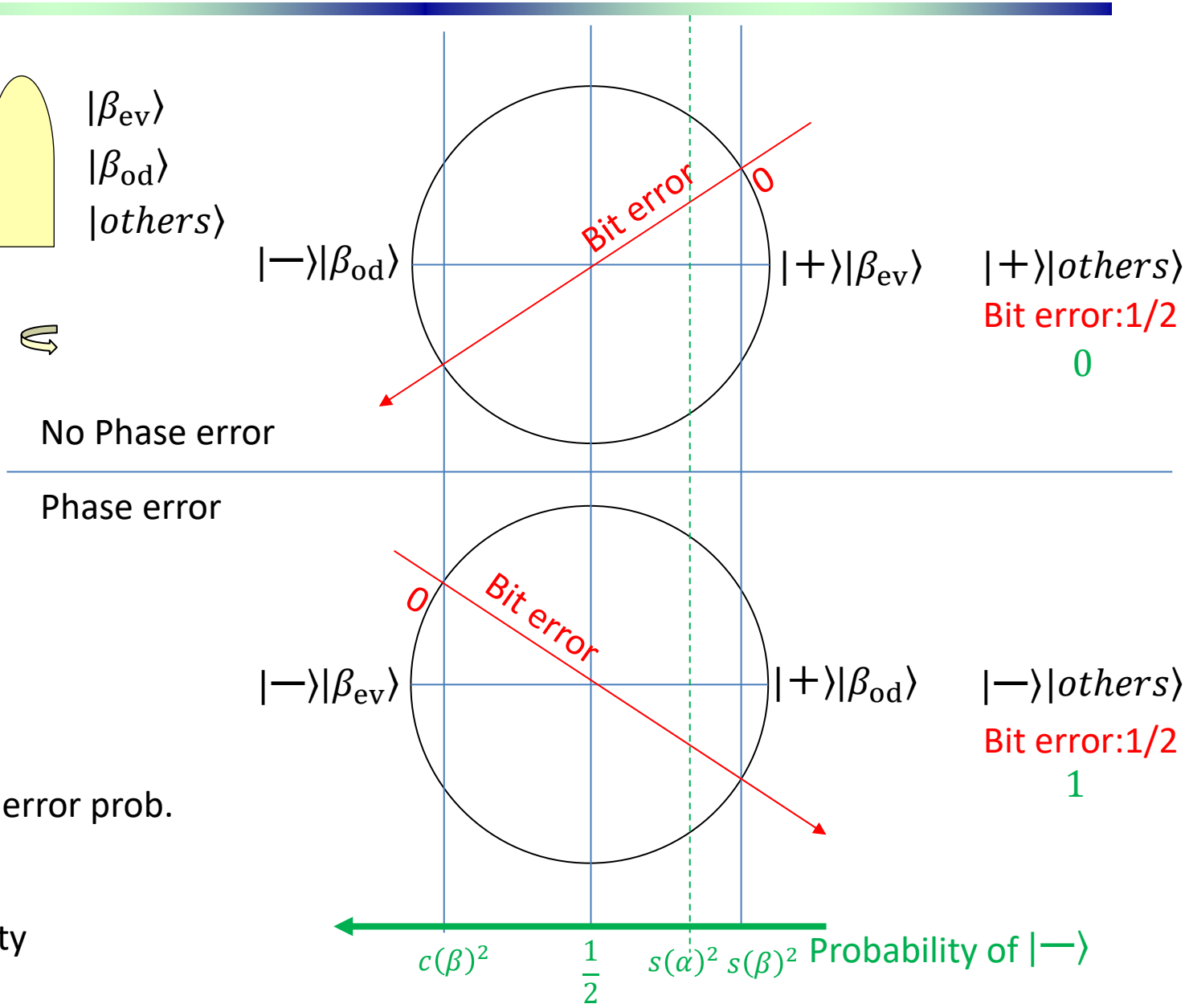
(consistent with beam splitting attack)

MK, *Phys. Rev. Lett.*, **93**, 120501 (2004)

B92 protocol: Analysis of phase error probability

Basis:





Asymptotic:

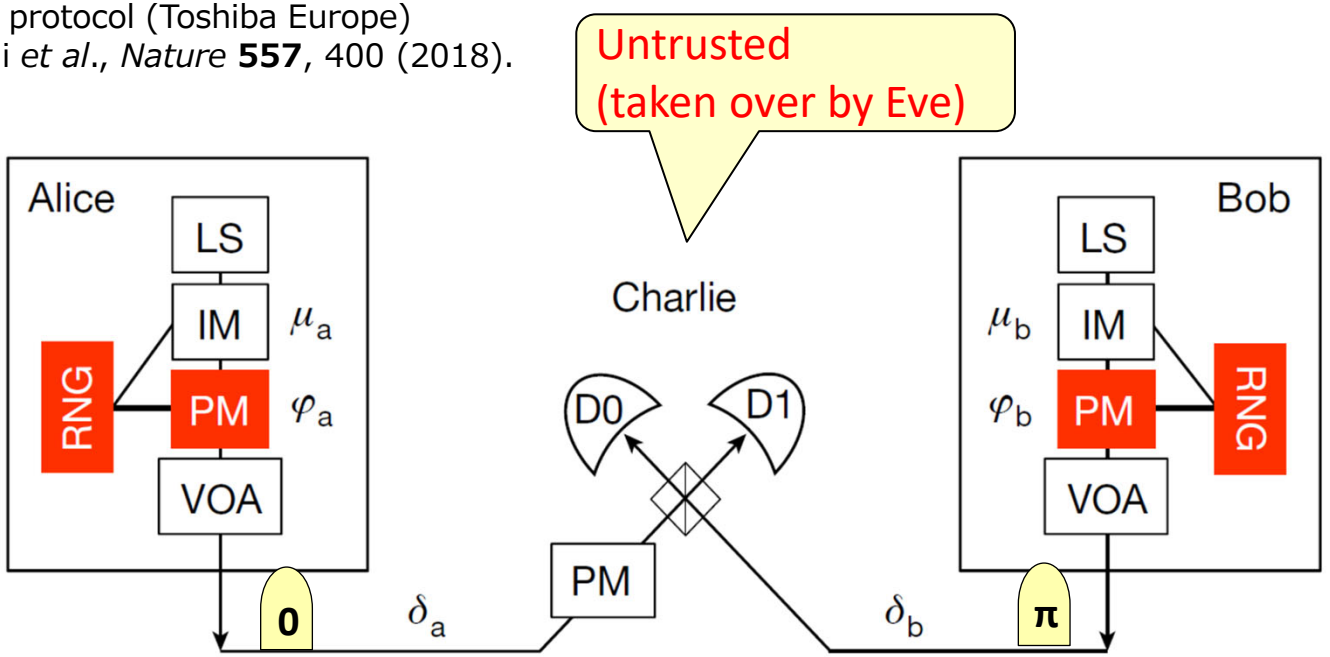
- Given
  - Bit error prob.
  - Detection prob.
- Compute
  - the worst phase error prob.

Finite-size:

- Azuma's inequality

Twin-Field QKD

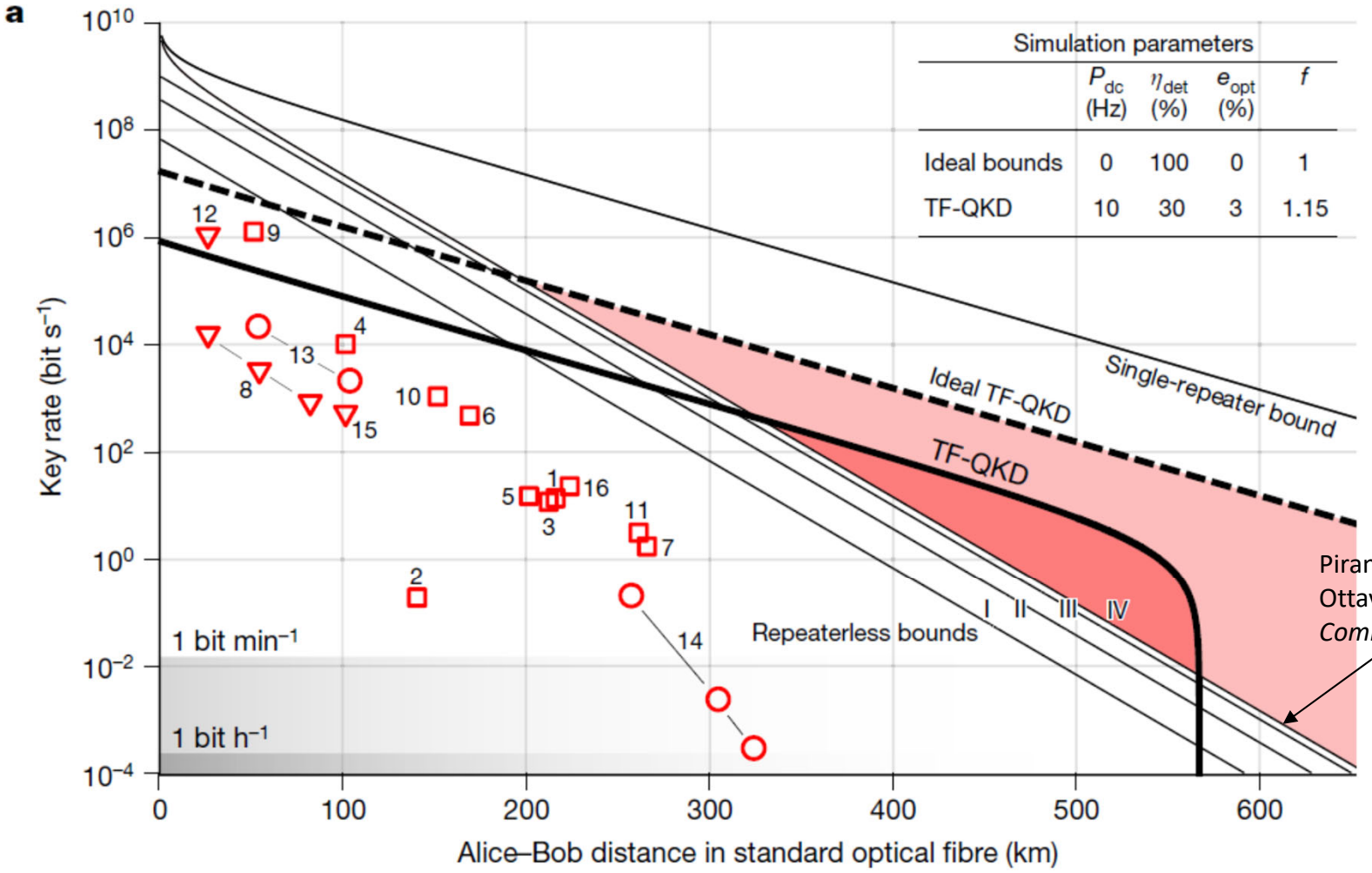
Twin-Field protocol (Toshiba Europe)
Lucamarini *et al*., *Nature* **557**, 400 (2018).



Only uses lasers, linear optics, and photon detectors.

Expected key rate scaling in TF-QKD

Twin-Field protocol (Toshiba Europe)
Lucamarini *et al*., *Nature* **557**, 400 (2018).

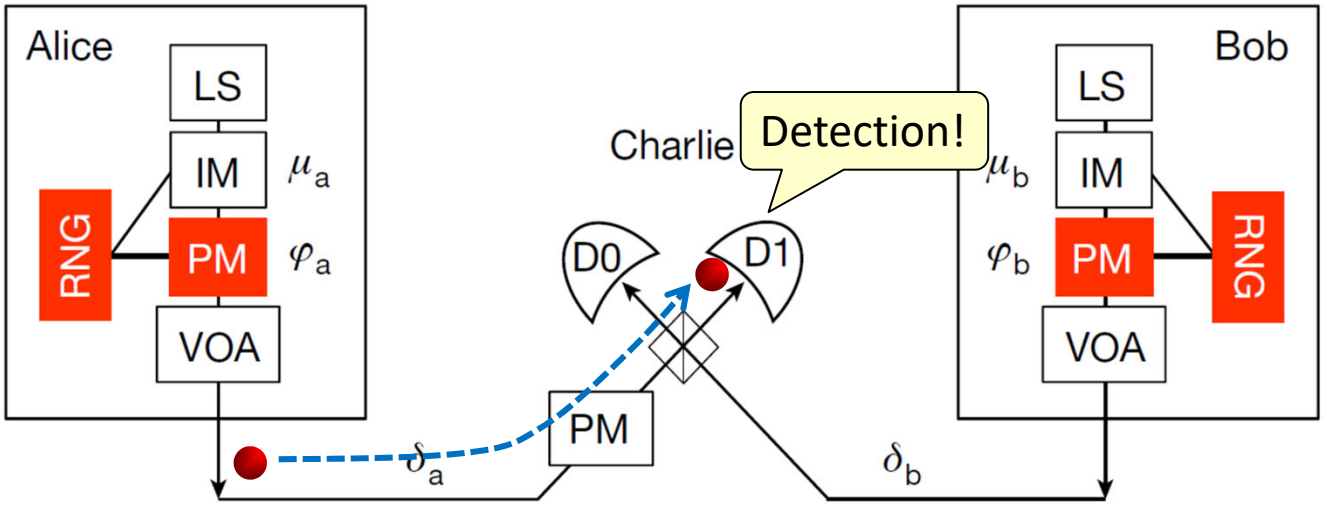


Pirandola, Laurenza, Ottaviani & Banchi., *Nat. Commun.* **8**, 15043 (2017).

It is expected that the achievable distance is doubled.

Twin-Field QKD

Twin-Field protocol (Toshiba Europe)
Lucamarini *et al*., *Nature* **557**, 400 (2018).

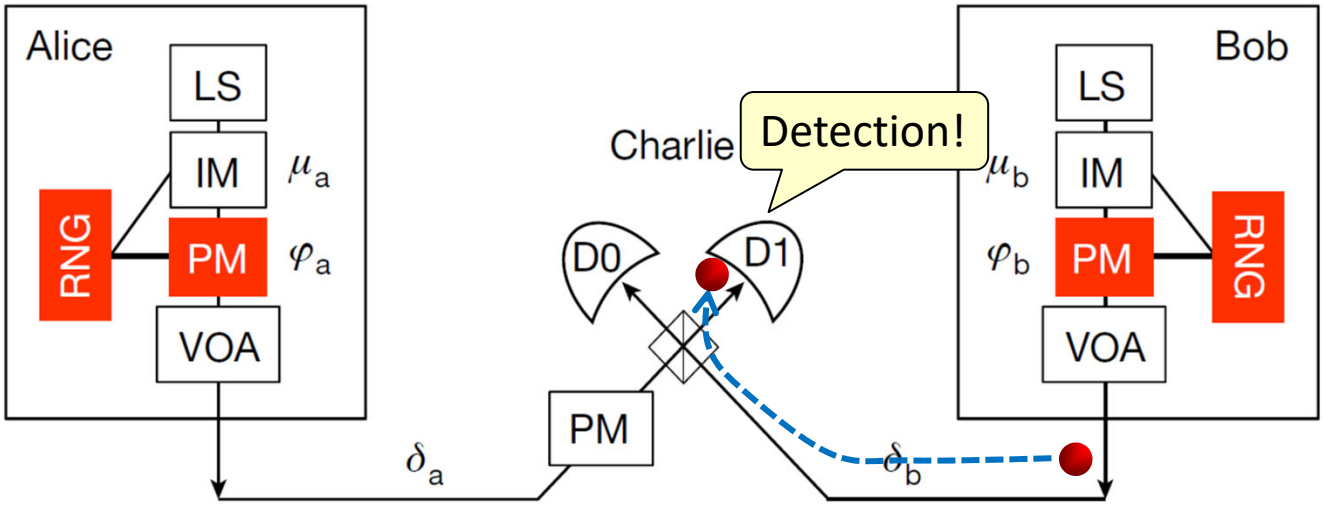


A photon travels only half the distance between Alice and Bob.

cf. A prepare-and-measure QKD

Twin-Field QKD

Twin-Field protocol (Toshiba Europe)
Lucamarini *et al*., *Nature* **557**, 400 (2018).



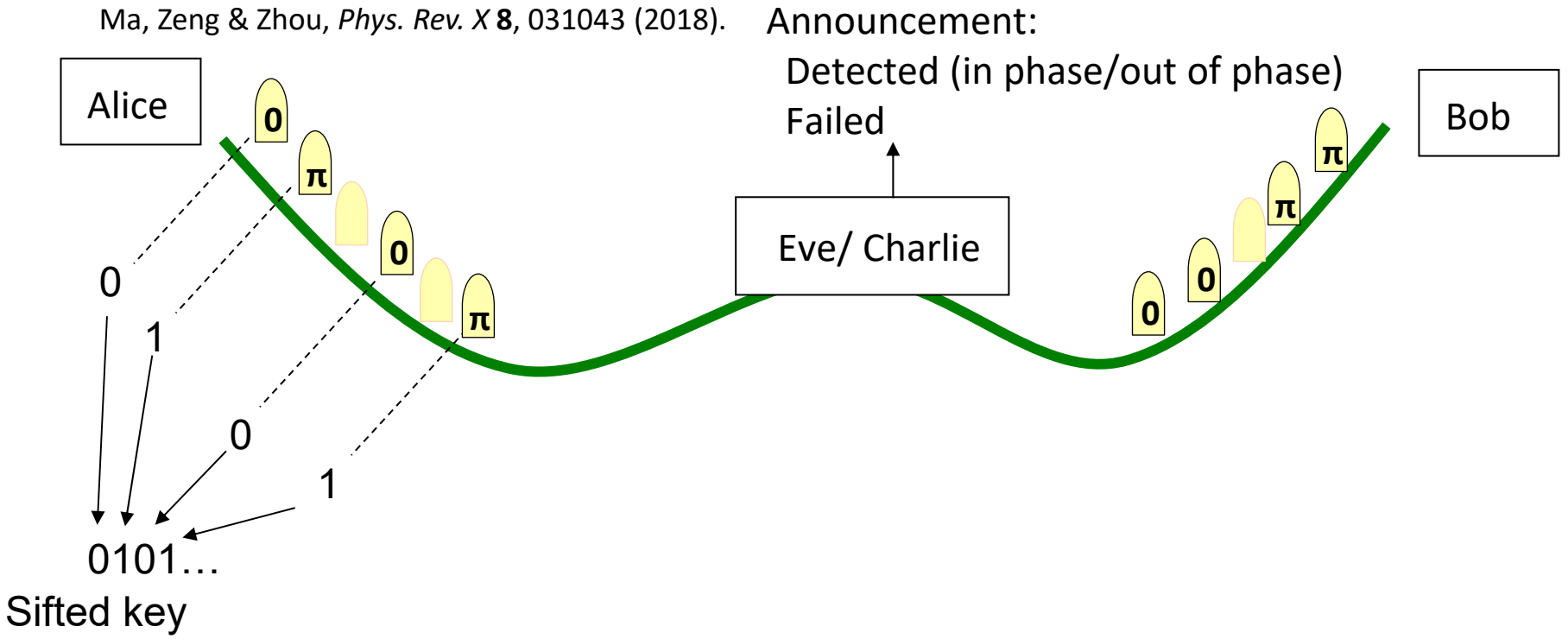
A photon travels only half the distance between Alice and Bob.

cf. A prepare-and-measure QKD

Twin-Field-type QKD

"Phase-Matching" protocol

Ma, Zeng & Zhou, *Phys. Rev. X* **8**, 031043 (2018).

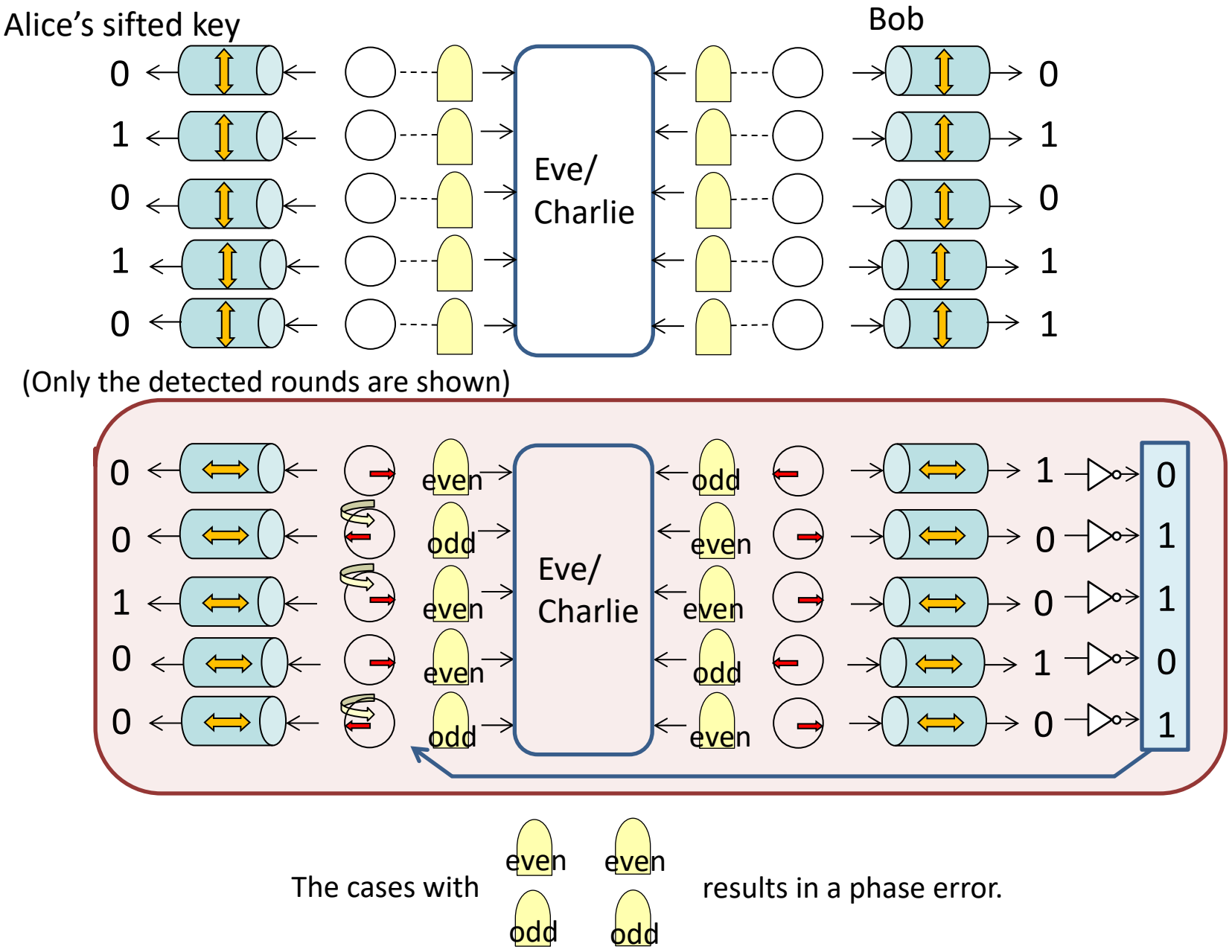


	Signal
0	0 $\lvert +\alpha\rangle$
1	π $\lvert -\alpha\rangle$

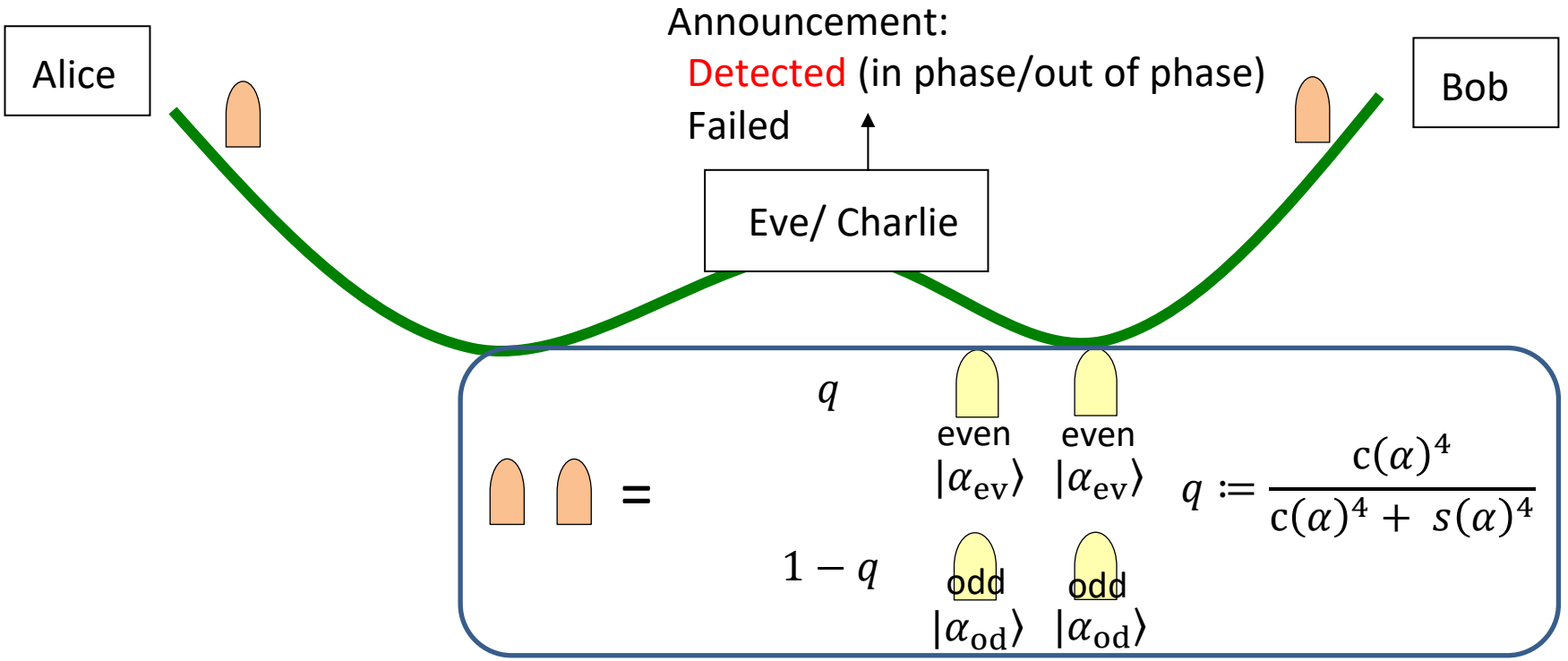
Test mode:

Many variants of PM protocols

TF-type QKD (PM protocol)



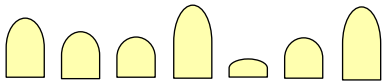
TF-type QKD (PM protocol)



Phase error probability ⇐ Estimation of detection rate of
(by only using coherent states)

	Signal	
0	0	$\lvert +\alpha\rangle$
1	π	$\lvert -\alpha\rangle$

Test mode:



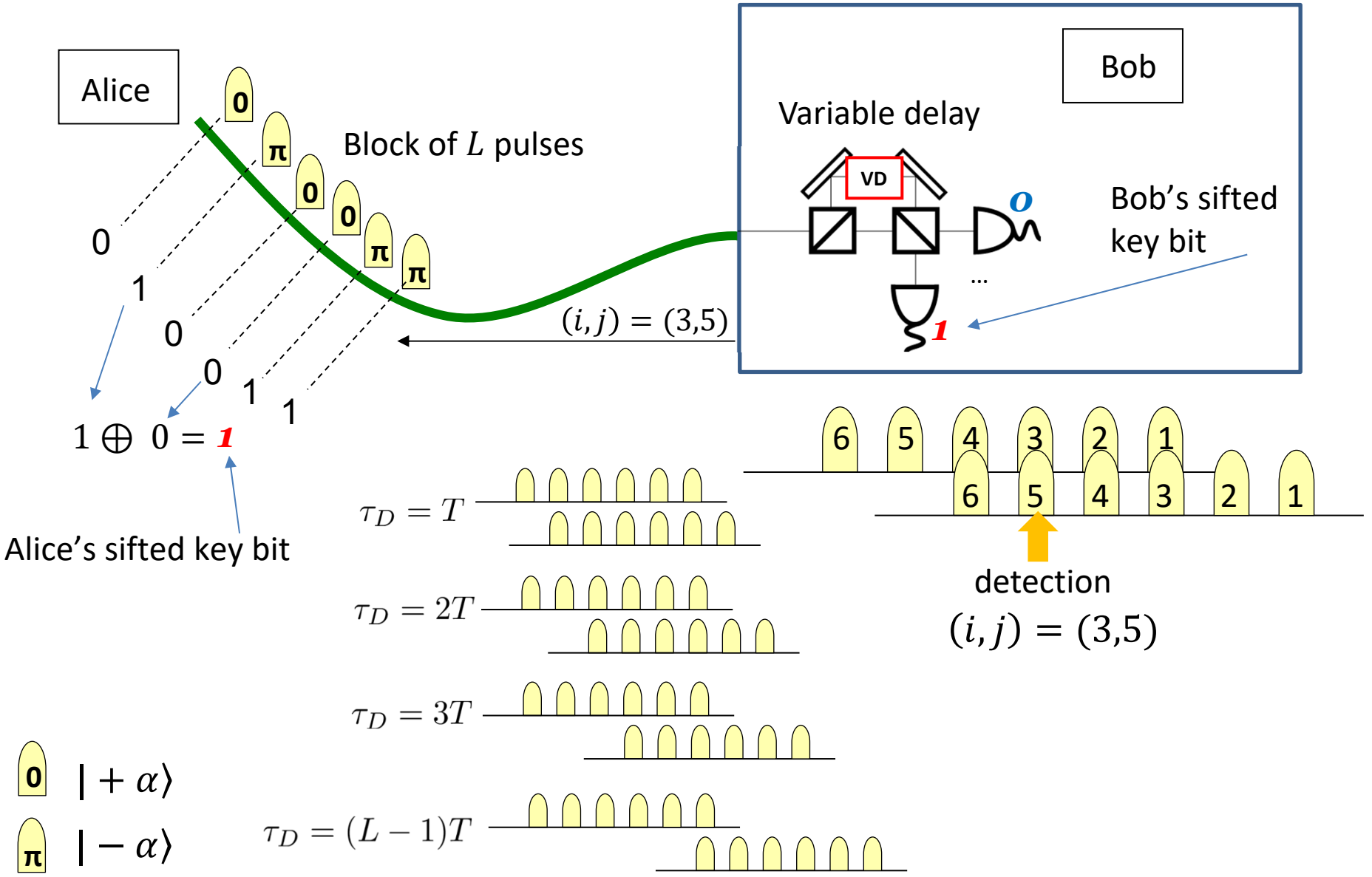
Asymptotic: Many designs proposed.

Finite-size:

- Reduction to Bernoulli sampling (Operation dominance method)[1)]
- (Improved version[3)] of) Azuma's inequality[2)]

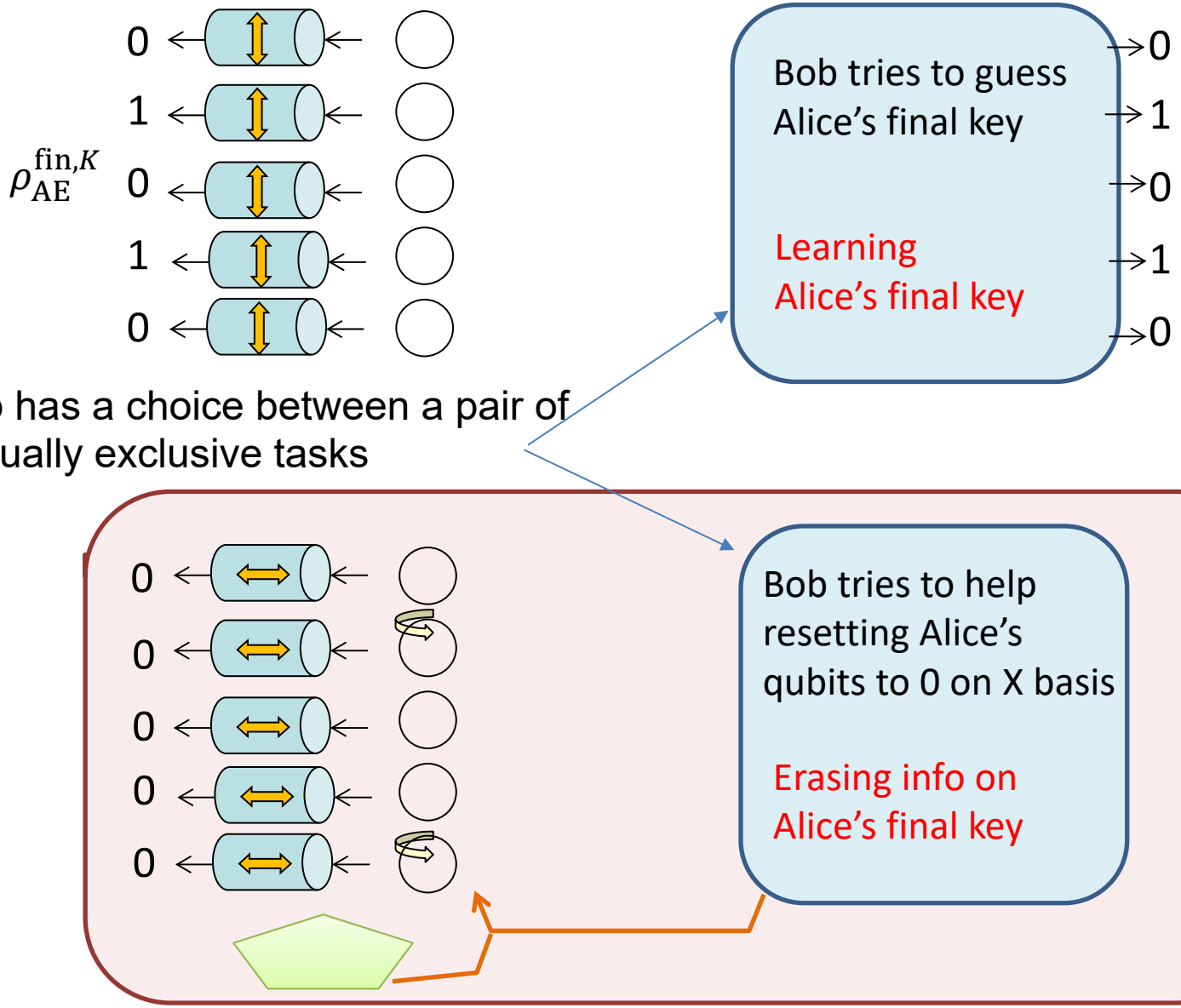
1) Maeda, Sasaki, MK, *Nat. Commun.* **10**, 3140 (2019). 2) Lorenzo, Navarrete, Azuma, Curty, Razavi, arXiv:1910.11407.
3) Kato, arXiv:2002.04357.

Round Robin DPS QKD

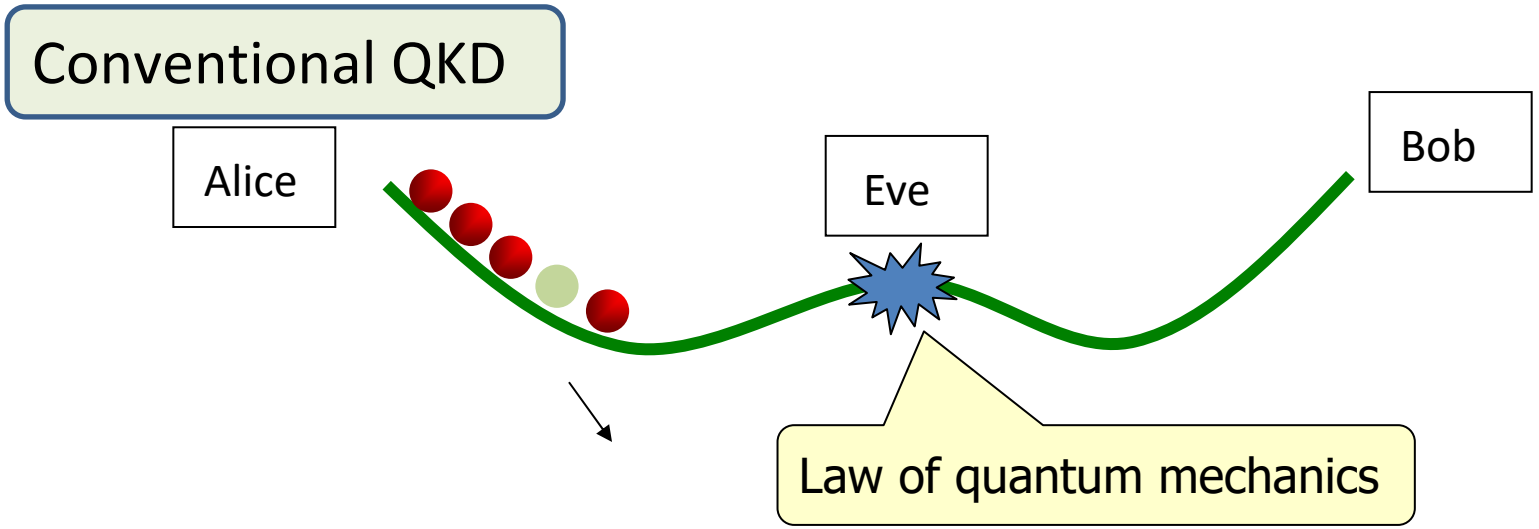


Sasaki, Yamamoto, MK, *Nature* **509**, 475 (2014).

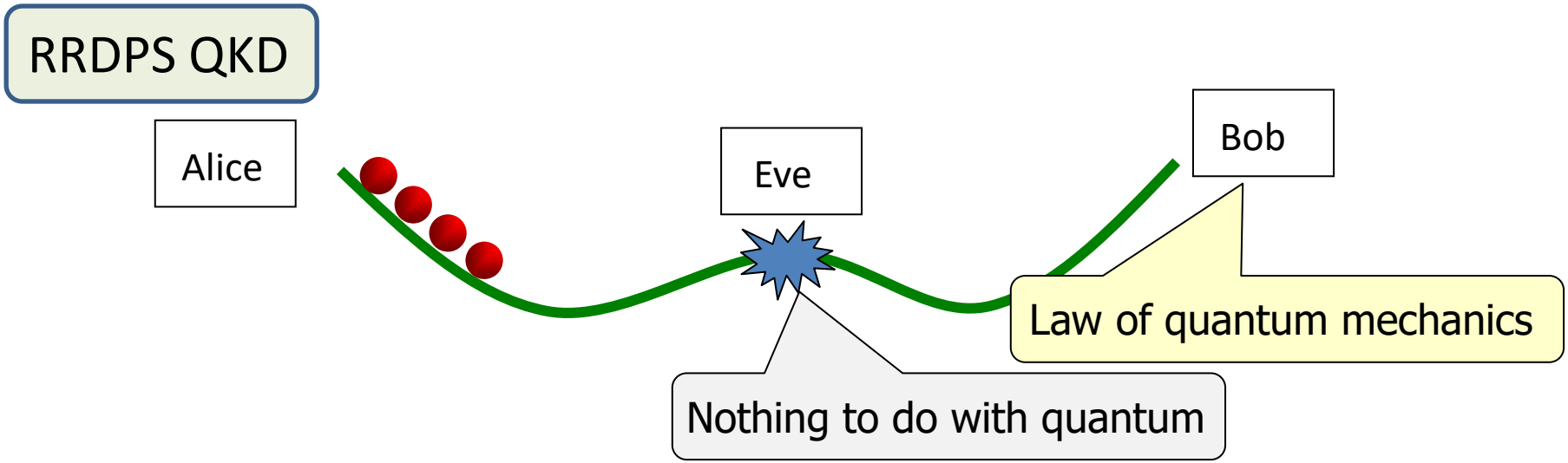
Security from complementarity



What is the working principle of QKD?

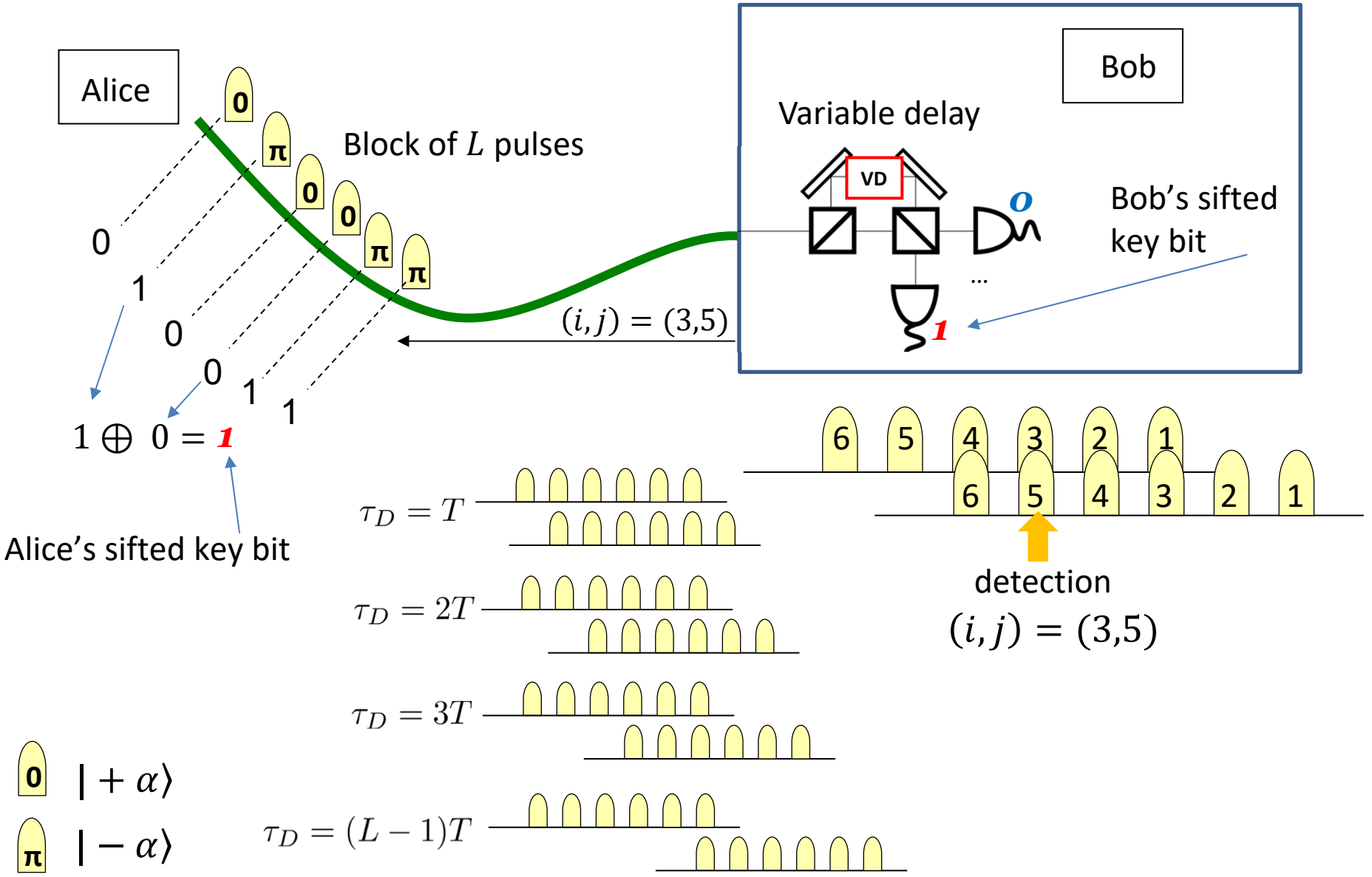


Eve's attempts to eavesdrop should leave a trace, which can be monitored.



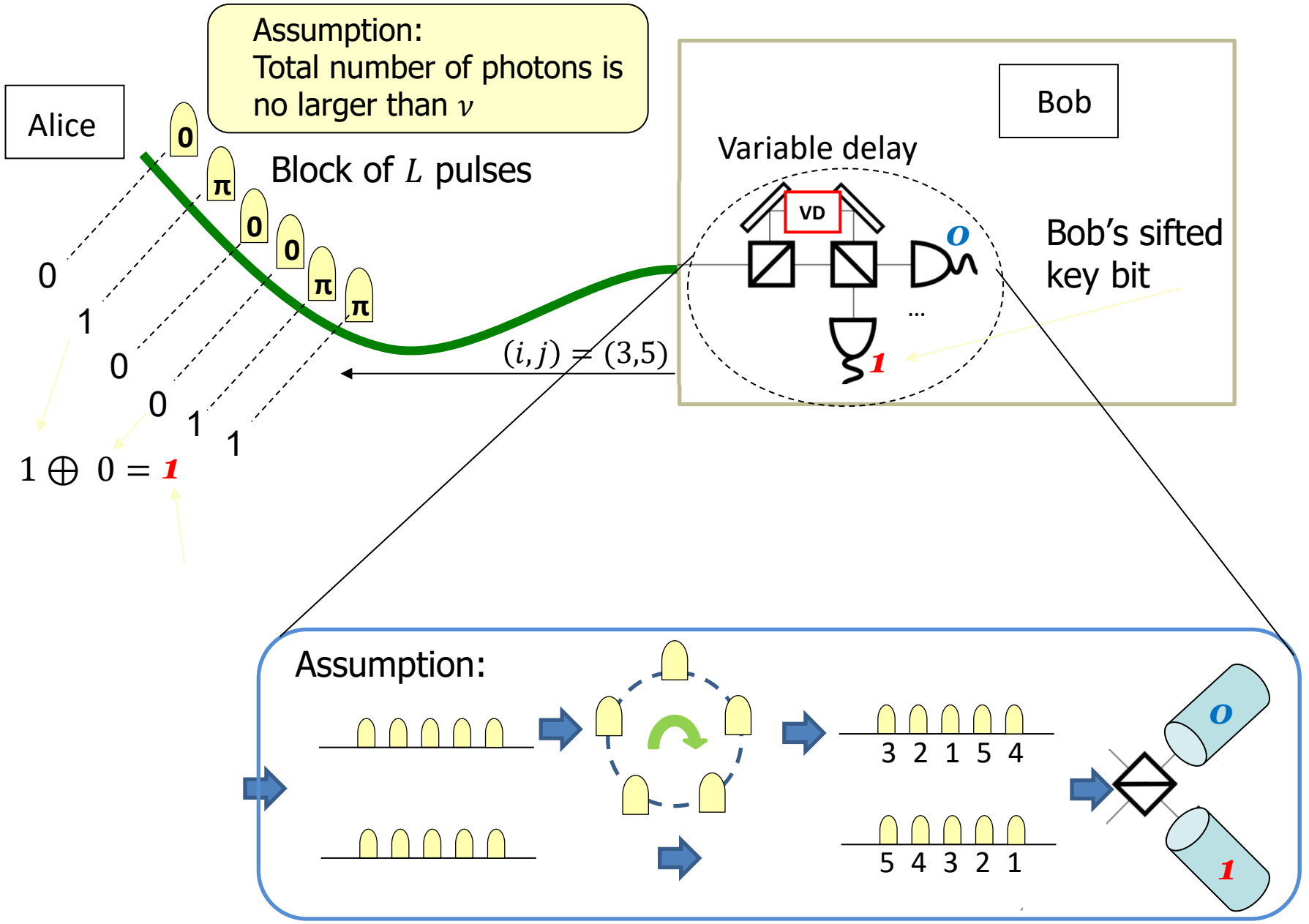
Eve has only a small chance to read out the bit, just because the signal is weak.

Round Robin DPS QKD

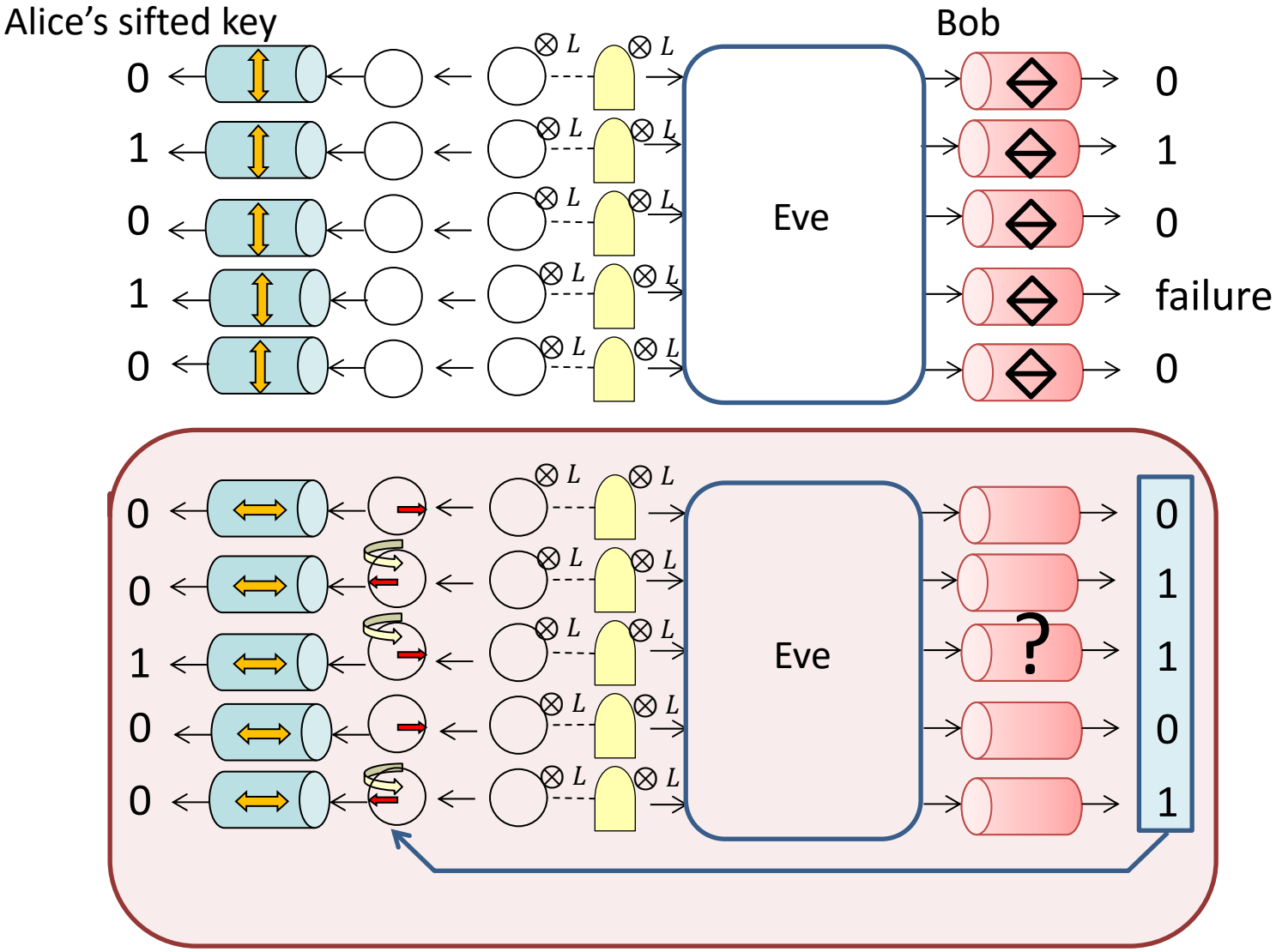


Sasaki, Yamamoto, MK, *Nature* **509**, 475 (2014).

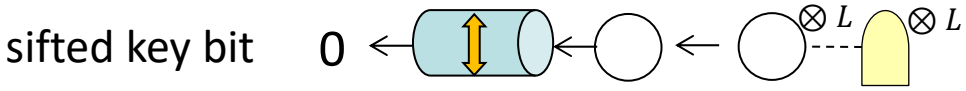
RRDPS QKD

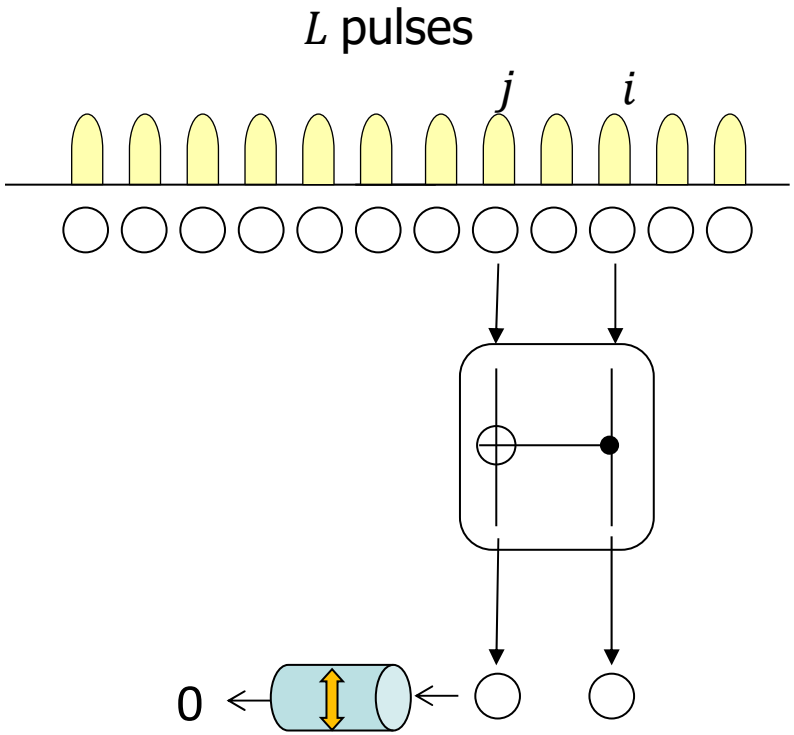

Assumption:
Total number of photons is no larger than ν
Alice
Block of L pulses
0
π
0
0
π
π
0
1
0
0
1
1
$1 \oplus 0 = 1$
$(i,j) = (3,5)$
Bob
Variable delay
VD
0
...
1
Bob's sifted key bit
Assumption:
3 2 1 5 4
5 4 3 2 1
0
1

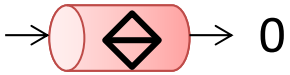
RRDPS protocol

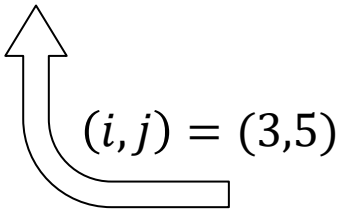


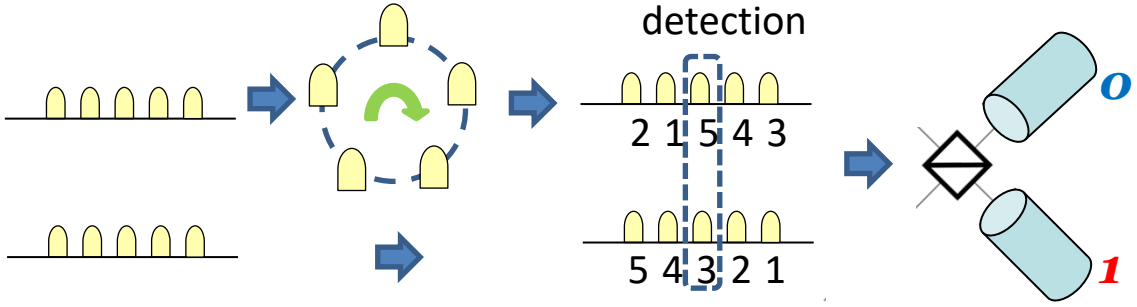
RRDPS QKD


sifted key bit
0
L
L

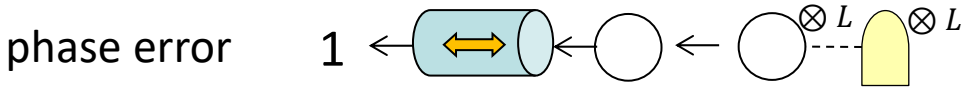

L pulses
j
i
0

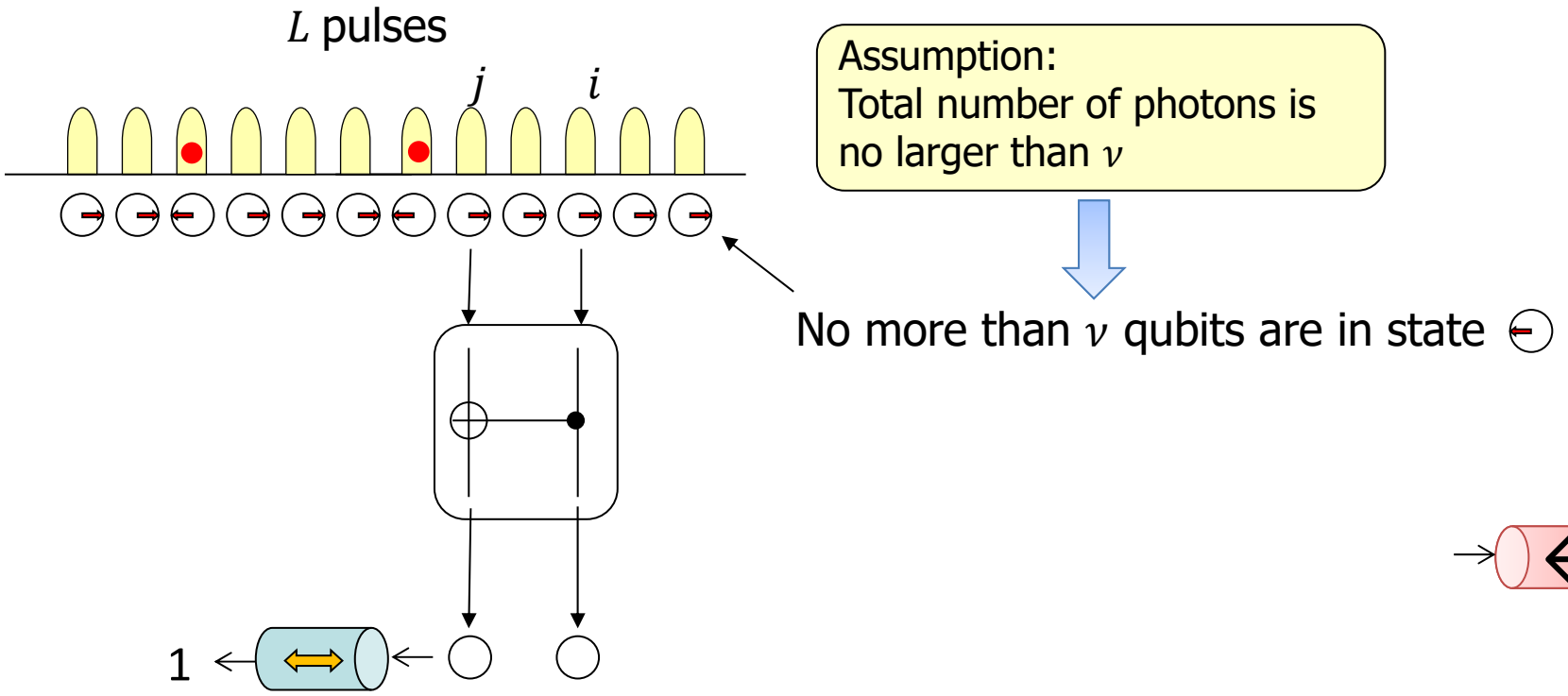

0

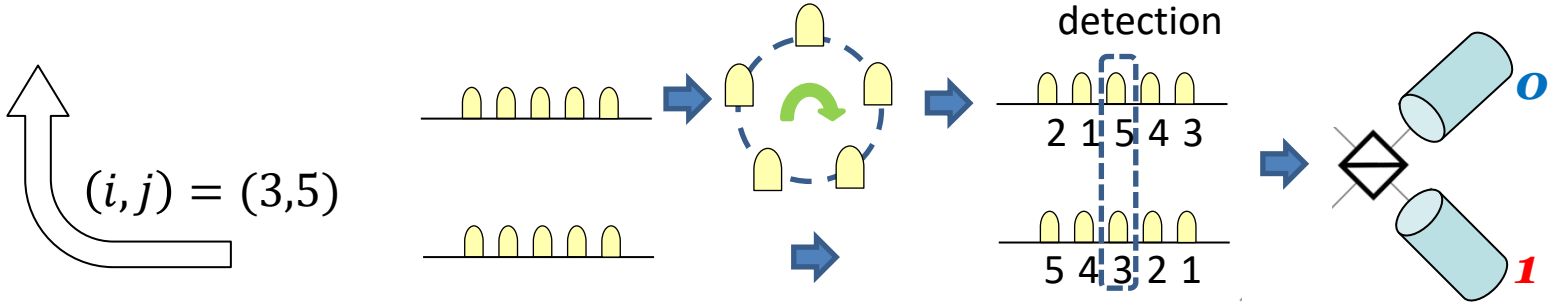

(i, j) = (3,5)


detection
2 1 5 4 3
5 4 3 2 1
0
1

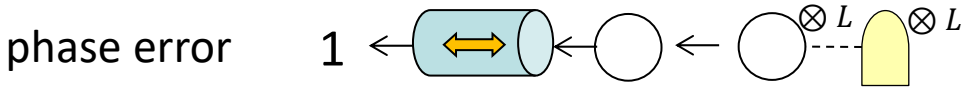
RRDPS QKD

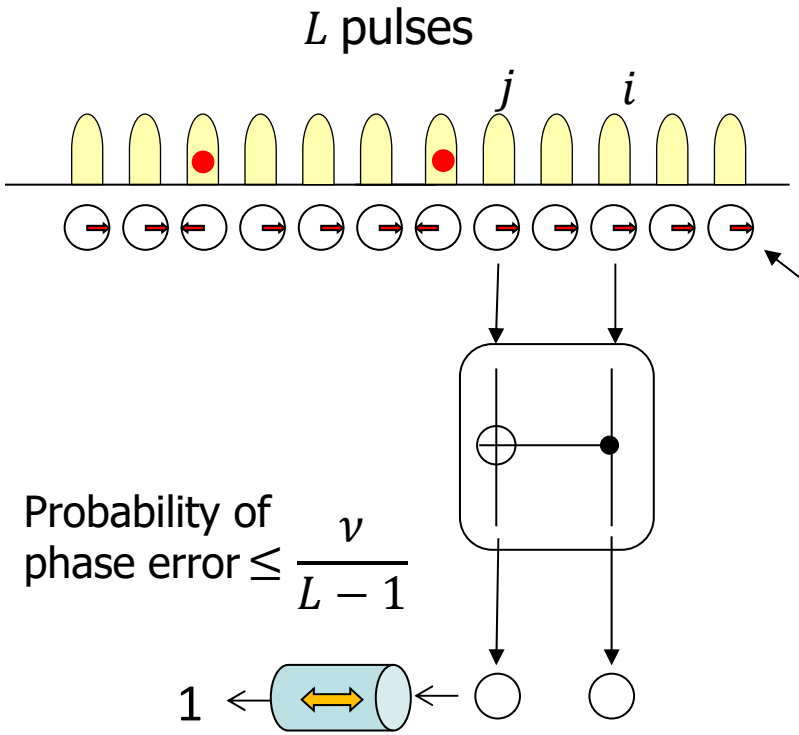

phase error
1
L
L


L pulses
j
i
Assumption:
Total number of photons is
no larger than ν
No more than ν qubits are in state
1
0


(i, j) = (3,5)
detection
2 1 5 4 3
5 4 3 2 1
0
1

RRDPS QKD

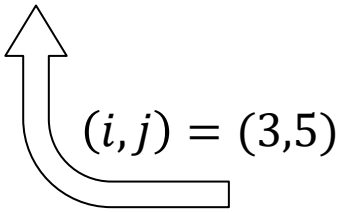


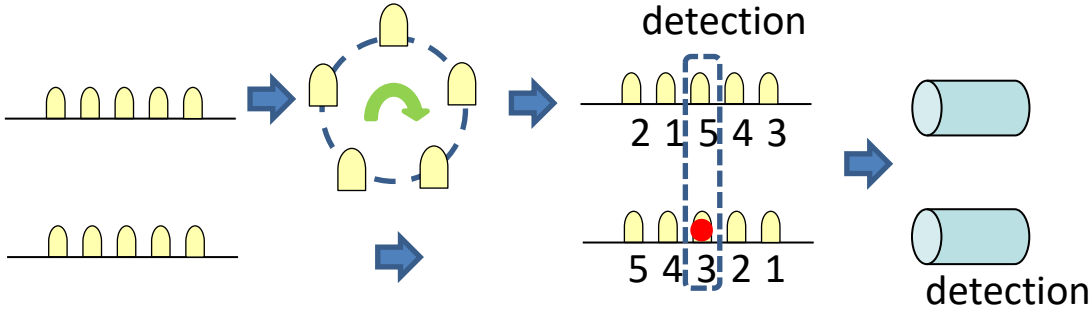


Assumption:
Total number of photons is no larger than ν

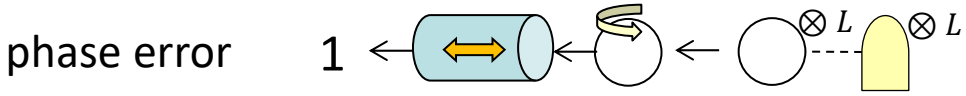
No more than ν qubits are in state ⊖

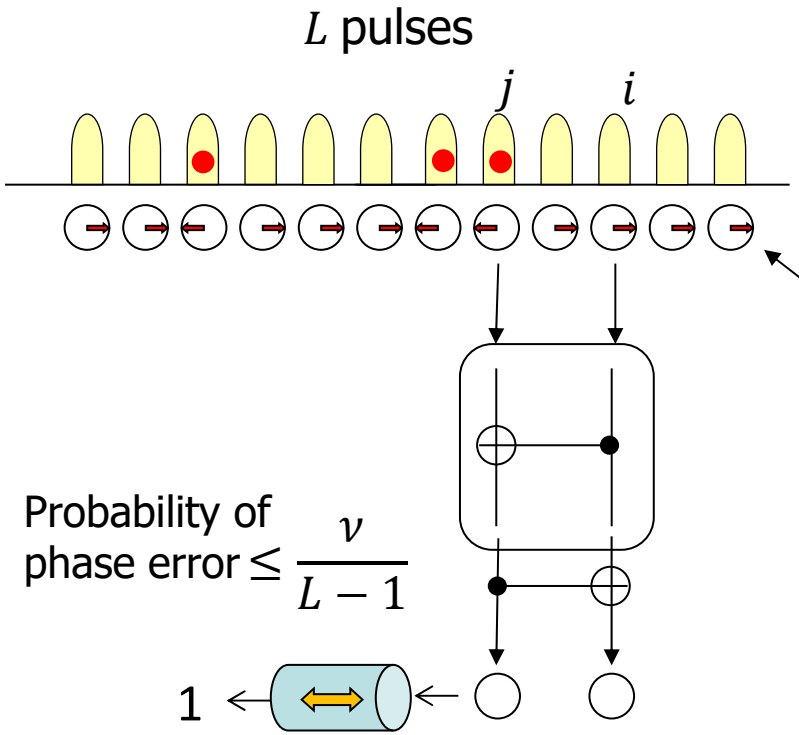
The index j is uniformly random.





RRDPS QKD

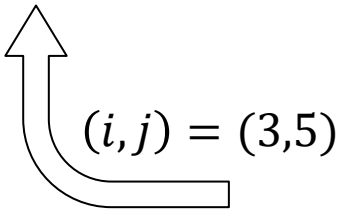


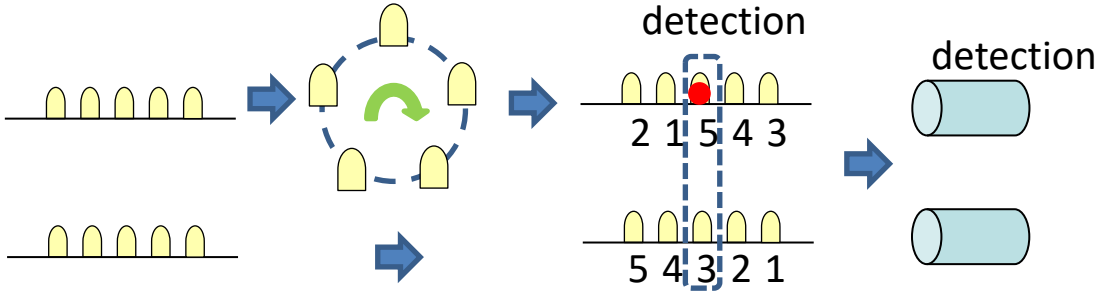


Assumption:
Total number of photons is no larger than ν

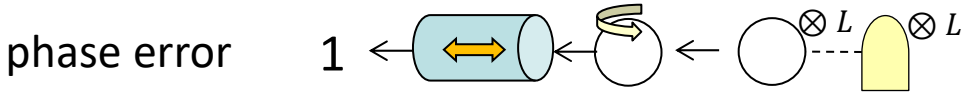
No more than ν qubits are in state ⊖

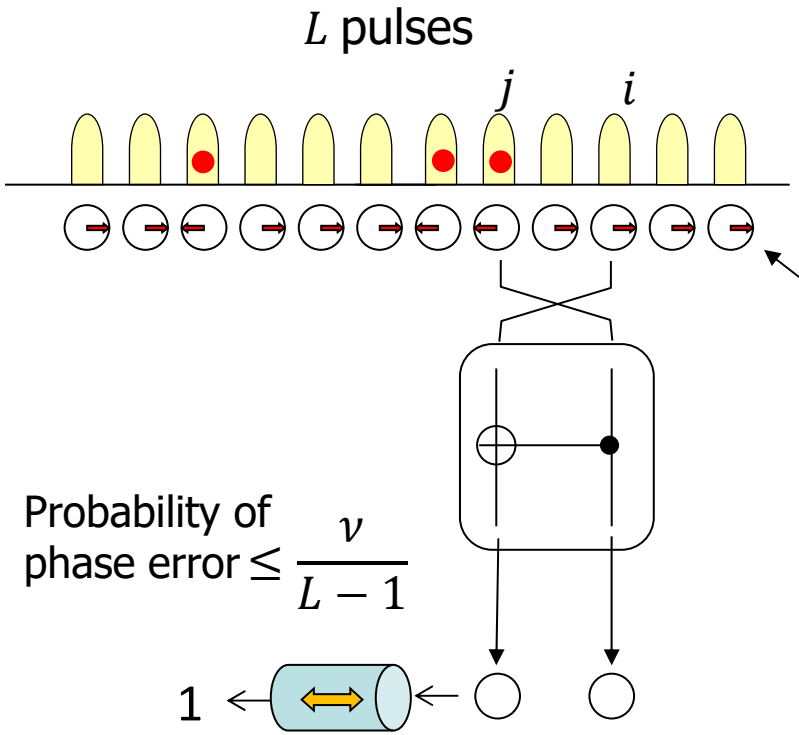
The index i is uniformly random.





RRDPS QKD

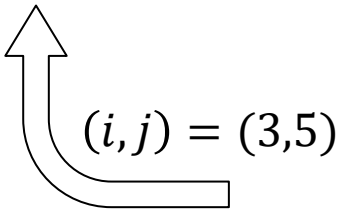


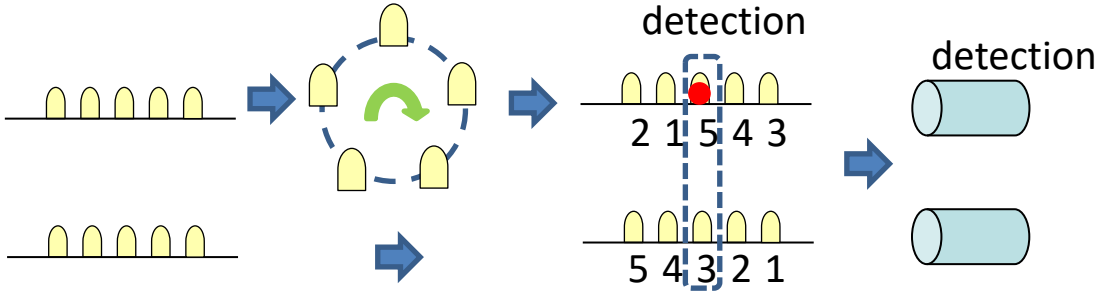


Assumption:
Total number of photons is no larger than ν

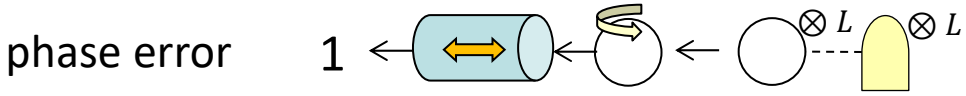
No more than ν qubits are in state 

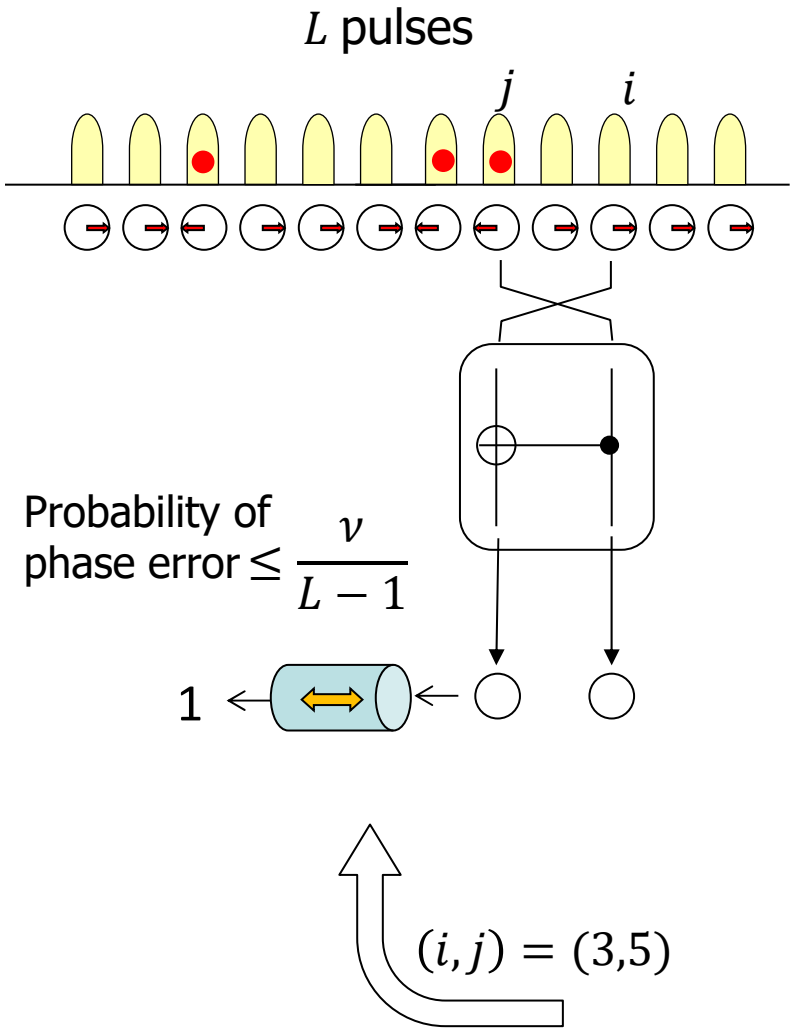
The index i is uniformly random.





RRDPS QKD

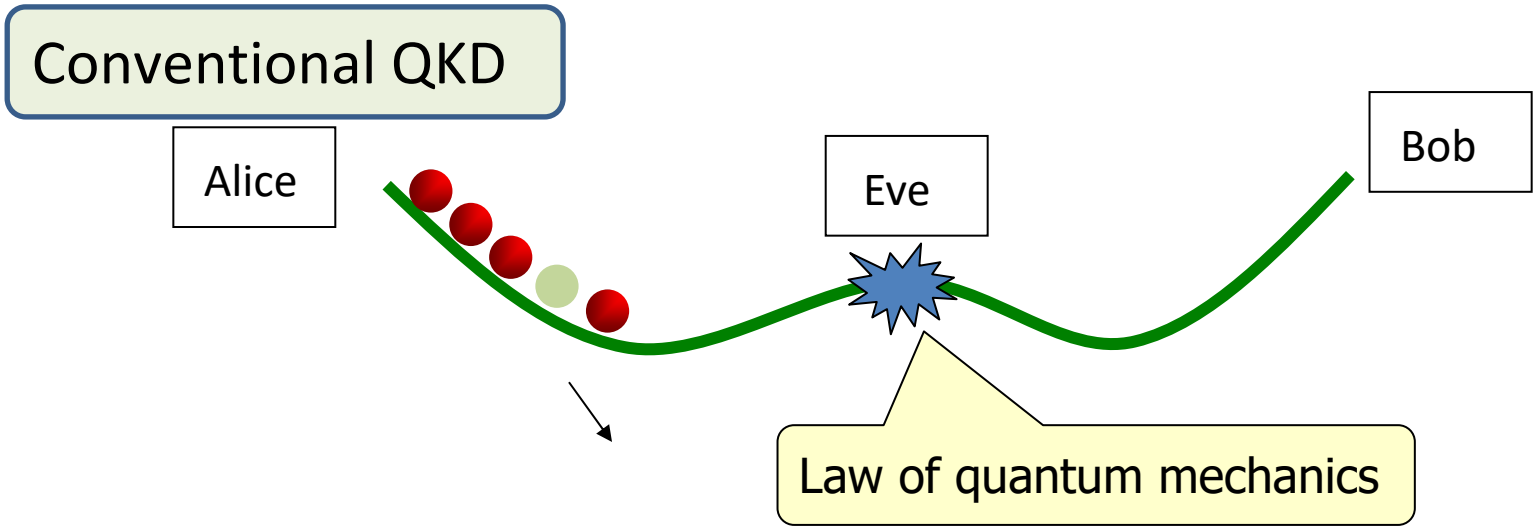




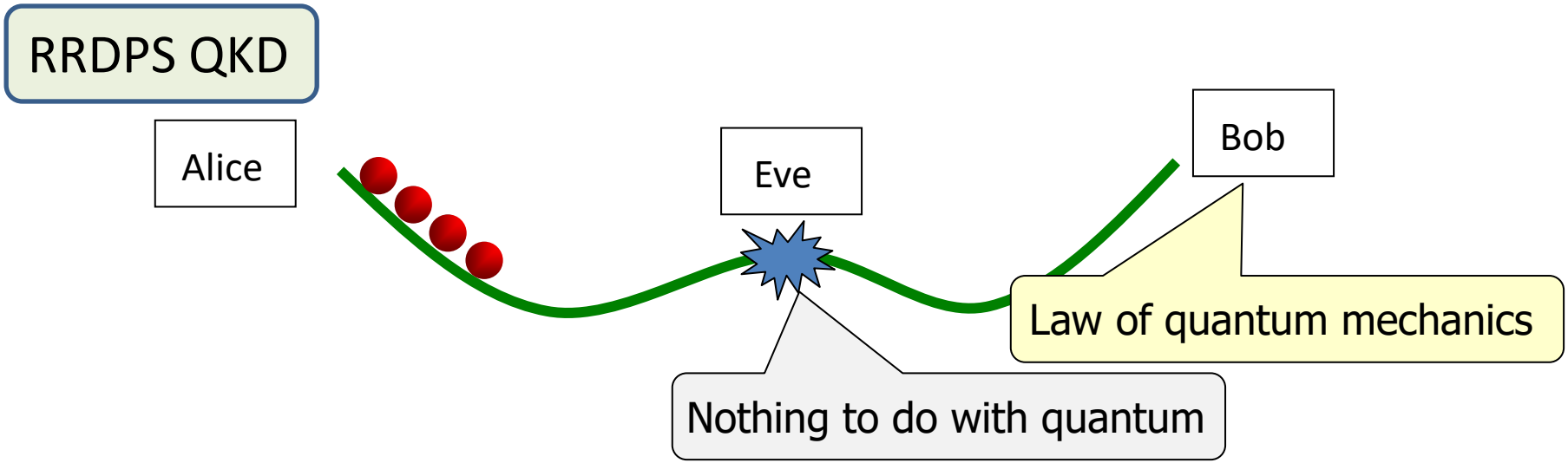
Asymptotic key length: $K \sim N - Nh(\frac{\nu}{L-1})$

Finite-size: No sampling needed.
Just a Bernoulli trial.

What is the working principle of QKD?



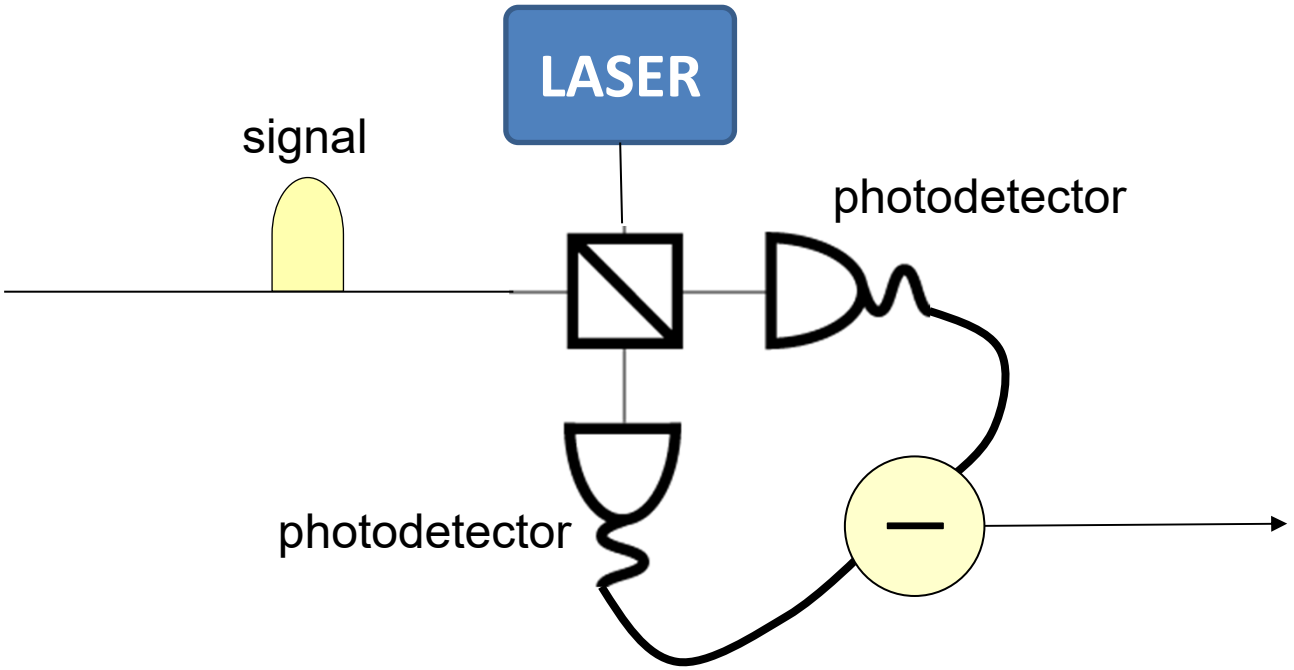
Eve's attempts to eavesdrop should leave a trace, which can be monitored.



Eve has only a small chance to read out the bit, just because the signal is weak.

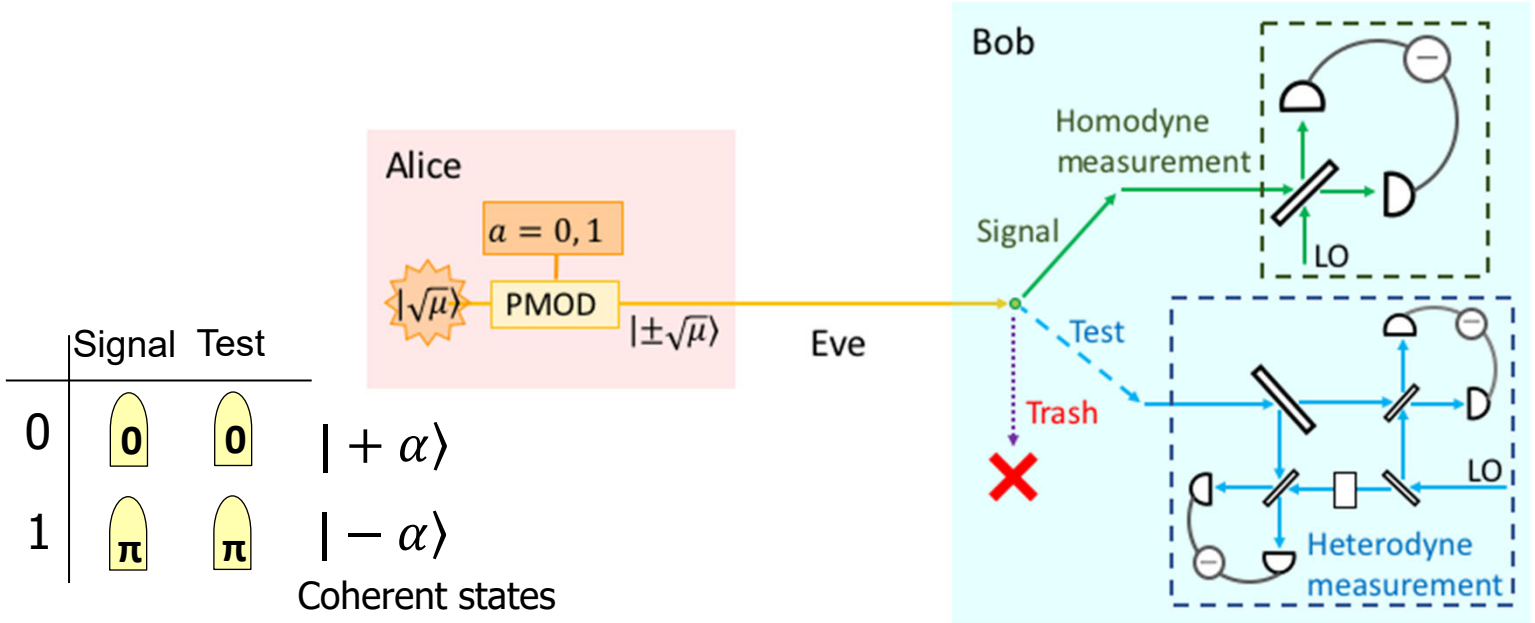
CV-QKD

Continuous-variable QKD
Homodyne/Heterodyne detection



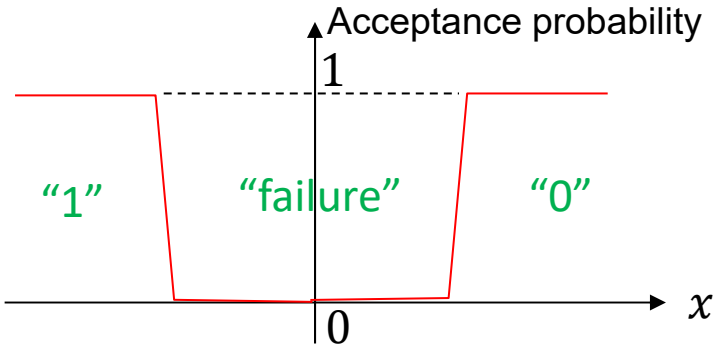
CV-QKD was off limits to the phase error approach.

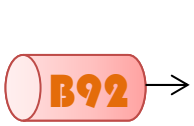
A two-state CV-QKD protocol



The B92 measurement has *two* roles.

Signal: Selecting out only favorable events.





0
1
failure

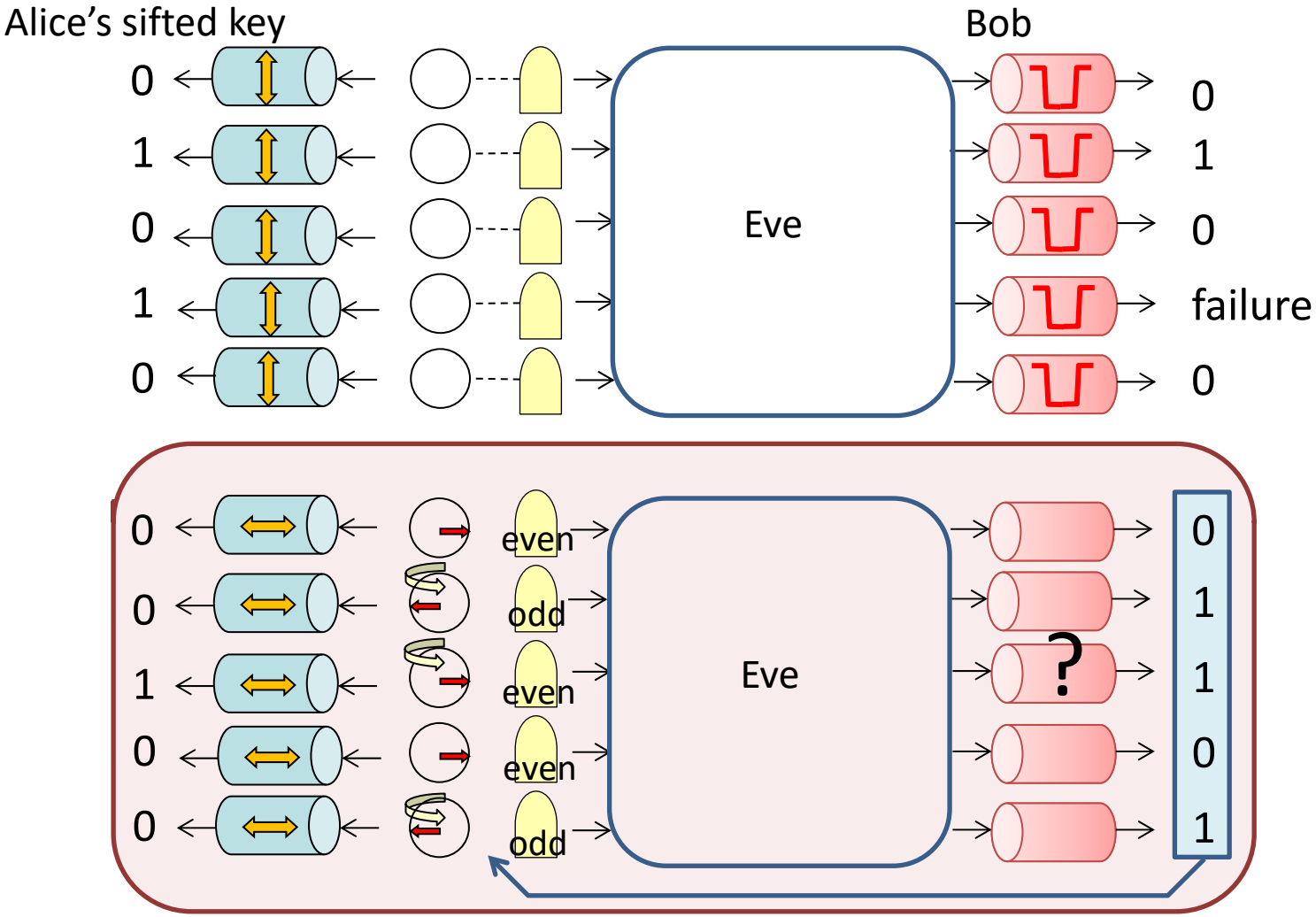
$$\beta := \sqrt{\eta}\alpha$$

Outcome 0: $\dfrac{1 - |-\beta\rangle\langle-\beta|}{2}$

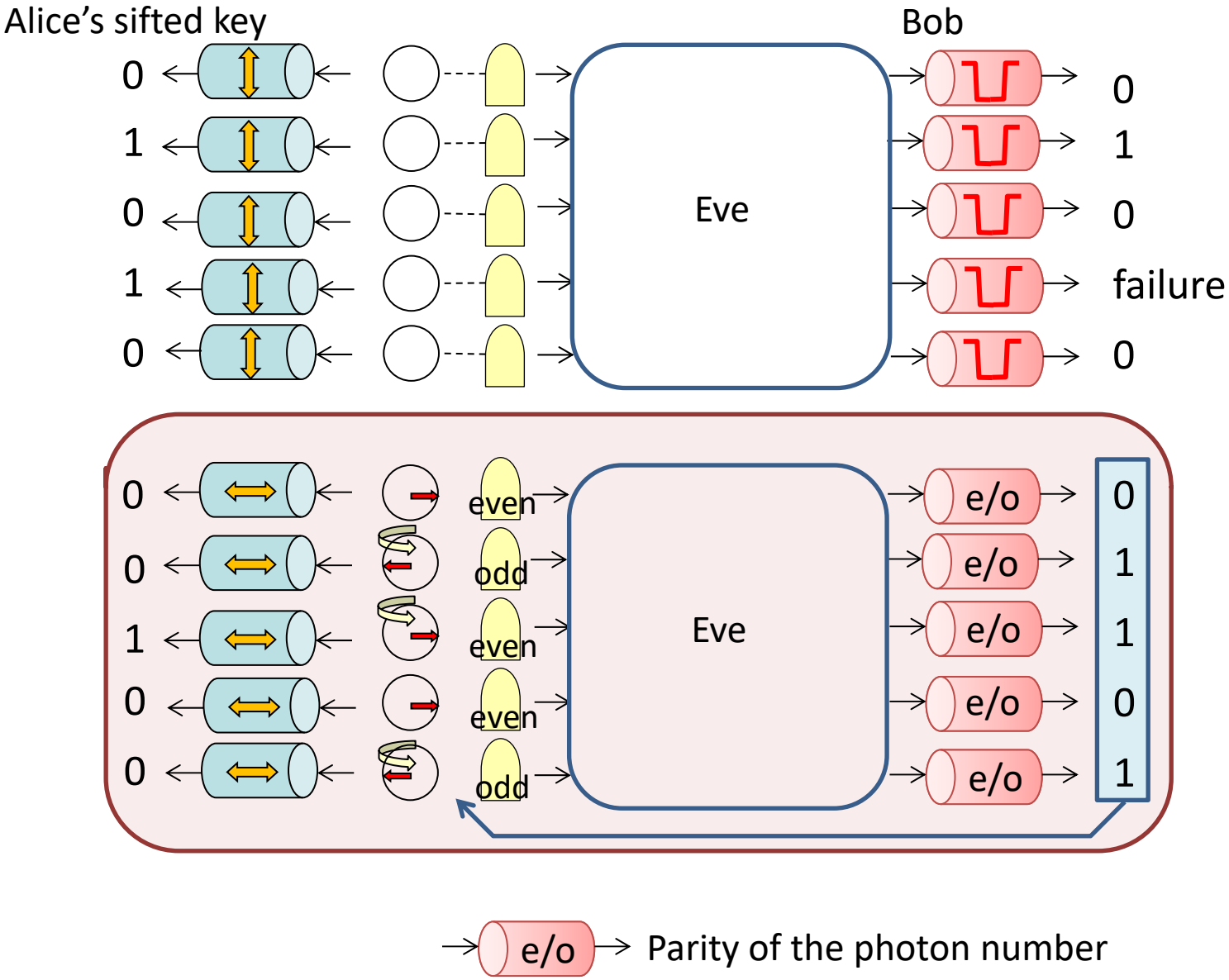
Outcome 1: $\dfrac{1 - |+\beta\rangle\langle+\beta|}{2}$

Matsuura, Maeda Sasaki, MK, arXiv: 2006.04661.

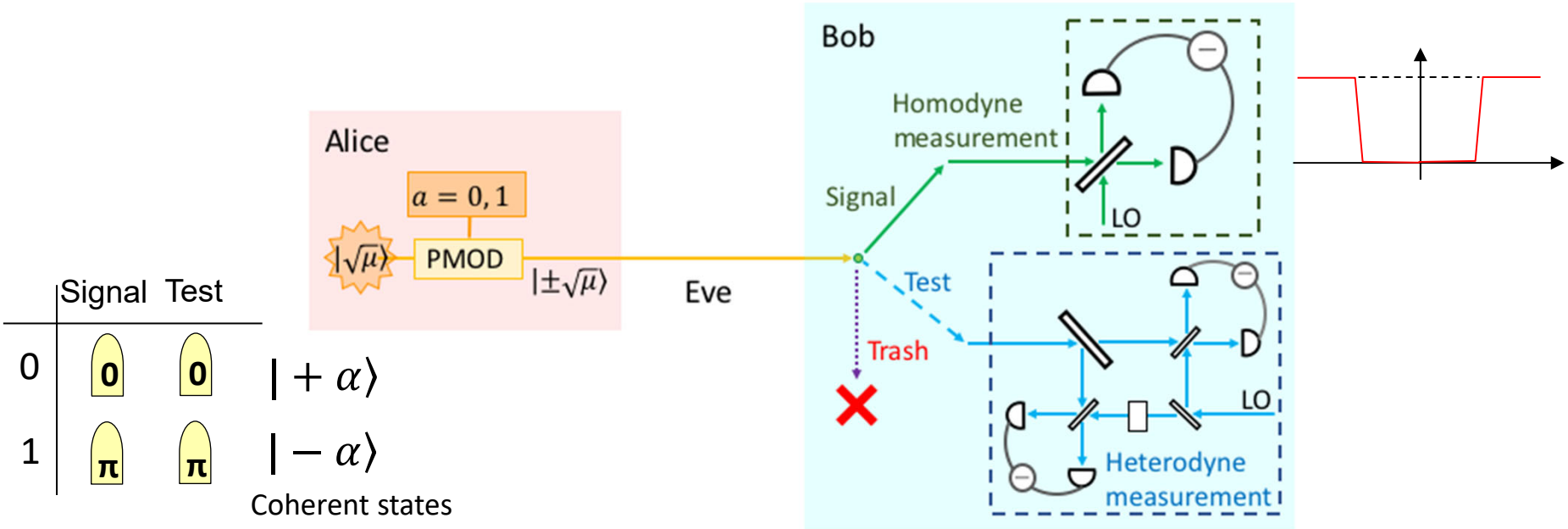
2-state CV protocol



2-state CV protocol



A two-state CV-QKD protocol



The B92 measurement has *two* roles.

Signal: Selecting out only favorable events.

Test: Estimation of bit error probability

⇩

Estimation of fidelities of the received state

$\langle+\beta|\rho_0|+\beta\rangle$ $\langle-\beta|\rho_1|-\beta\rangle$

B92 → 0, 1, failure

$\beta := \sqrt{\eta}\alpha$

Outcome 0: $\dfrac{1-|-\beta\rangle\langle-\beta|}{2}$

Outcome 1: $\dfrac{1-|+\beta\rangle\langle+\beta|}{2}$

Matsuura, Maeda Sasaki, MK, arXiv: 2006.04661.

Fidelity estimation via Heterodyne measurement

$$\Lambda_{m,r}(\mu) \coloneqq e^{-r\mu}(1+r)L_m^{(1)}((1+r)\mu)$$

m: odd integer

Associated Laguerre polynomial

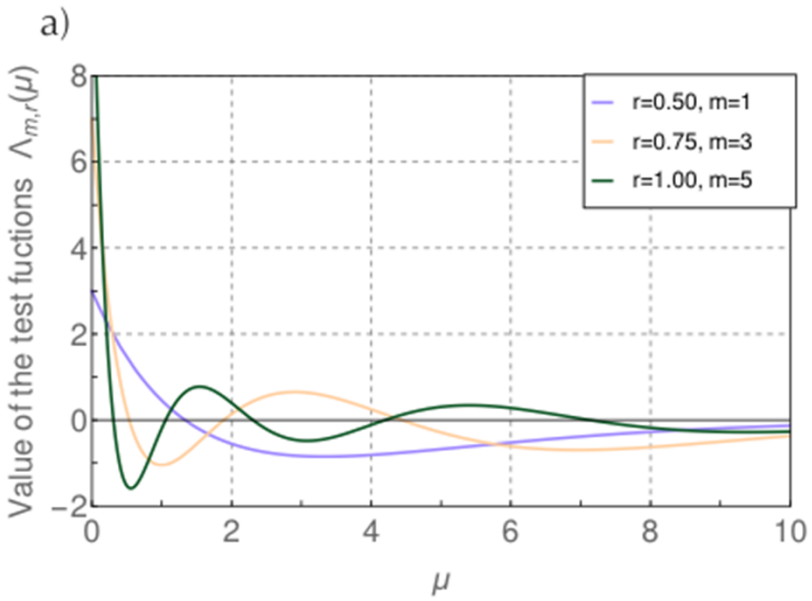
$\hat{\omega} \in \mathbb{C}$: Outcome of Heterodyne measurement

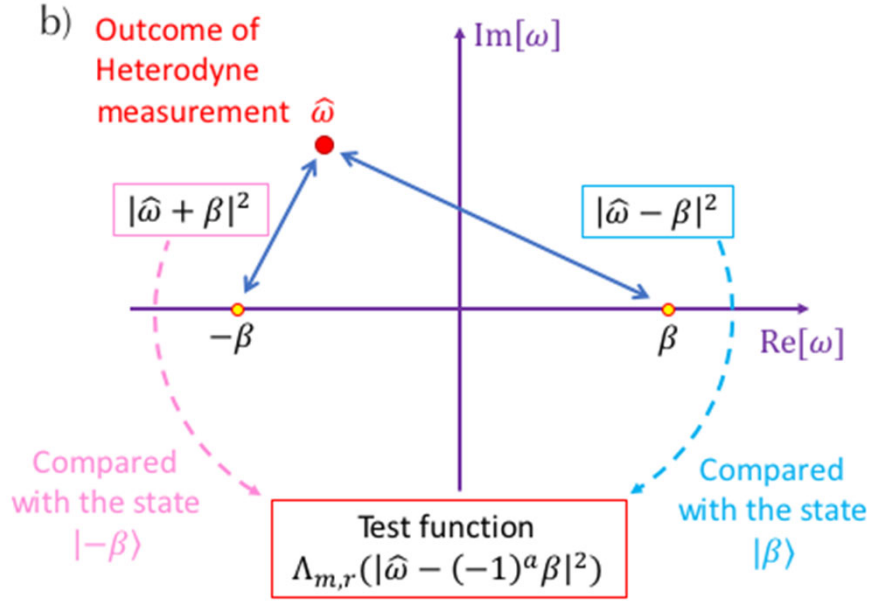
ρ: input state

$$\mathbb{E}_\rho[\Lambda_{m,r}(|\hat{\omega}|^2)] \leq \langle 0|\rho|0\rangle$$

The equality holds when ρ has m or fewer photons.

$$\mathbb{E}_\rho[\Lambda_{m,r}(|\hat{\omega} \pm \beta|^2)] \leq \langle \pm\beta|\rho|\pm\beta\rangle$$





Matsuura, Maeda Sasaki, MK, arXiv: 2006.04661.

Security proof of 2-state CV-QKD

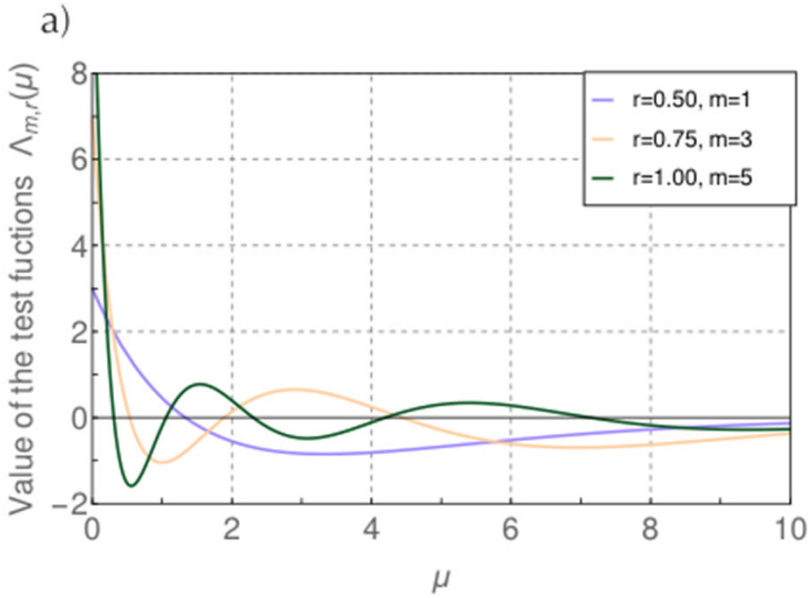
$\Lambda_{m,r}(\mu)$ is bounded and smooth

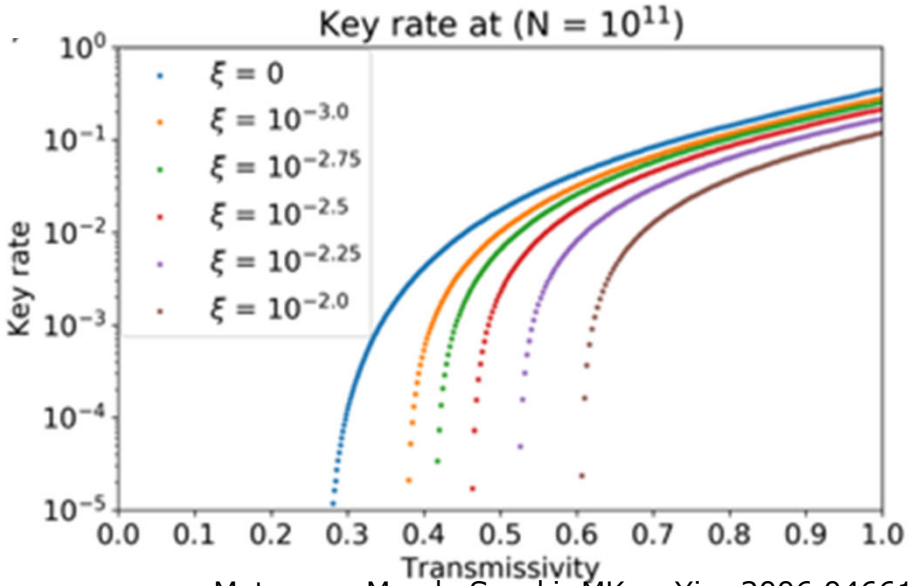
✓ Finite-size security
(Azuma's inequality)

✓ Against general attack

✓ Finite measurement precision

✓ Finite constellation





Matsuura, Maeda Sasaki, MK, arXiv: 2006.04661.