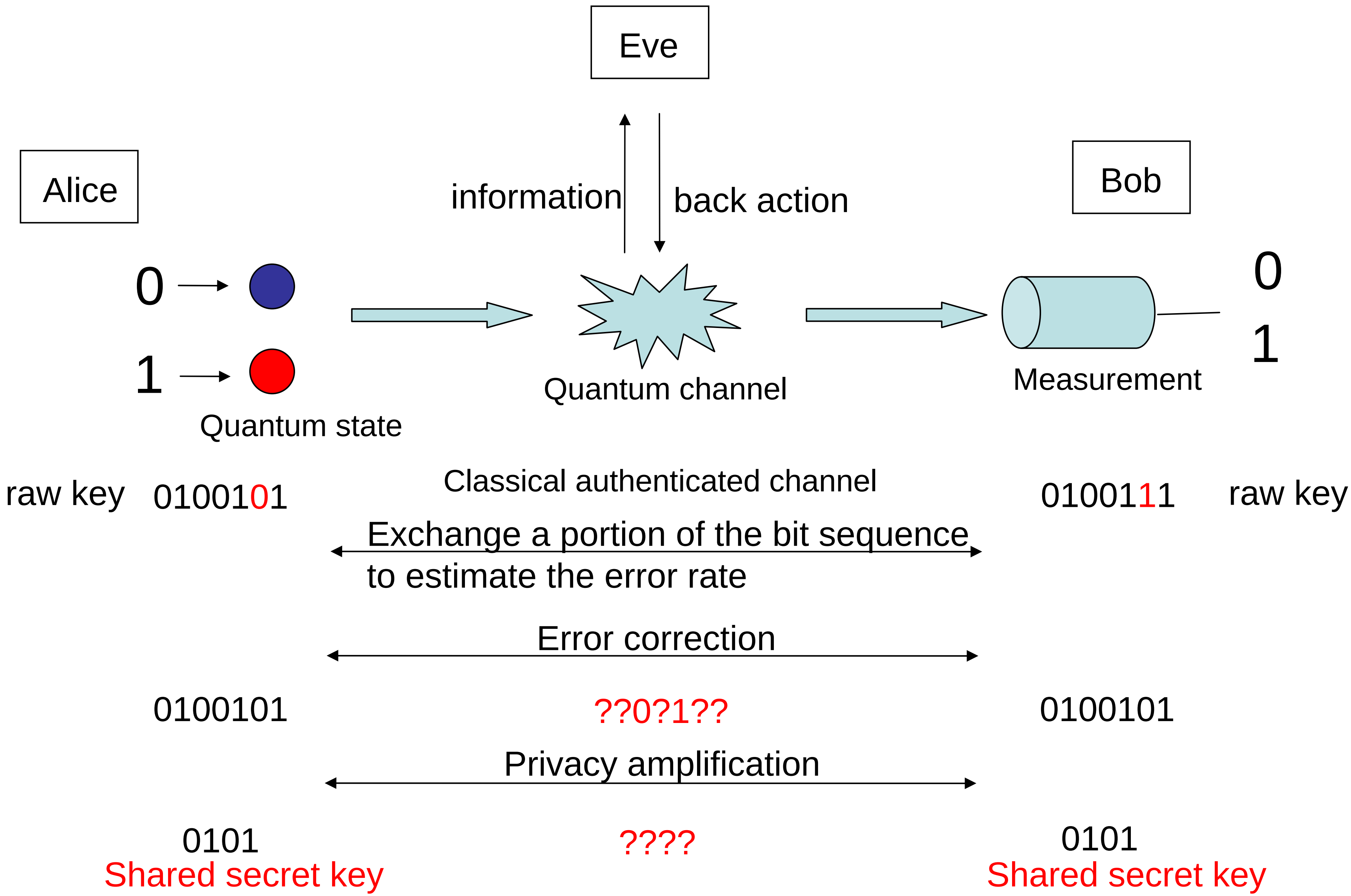
量子暗号の安全性と量子系の基本的性質

小芦　雅斗

阪大基礎工

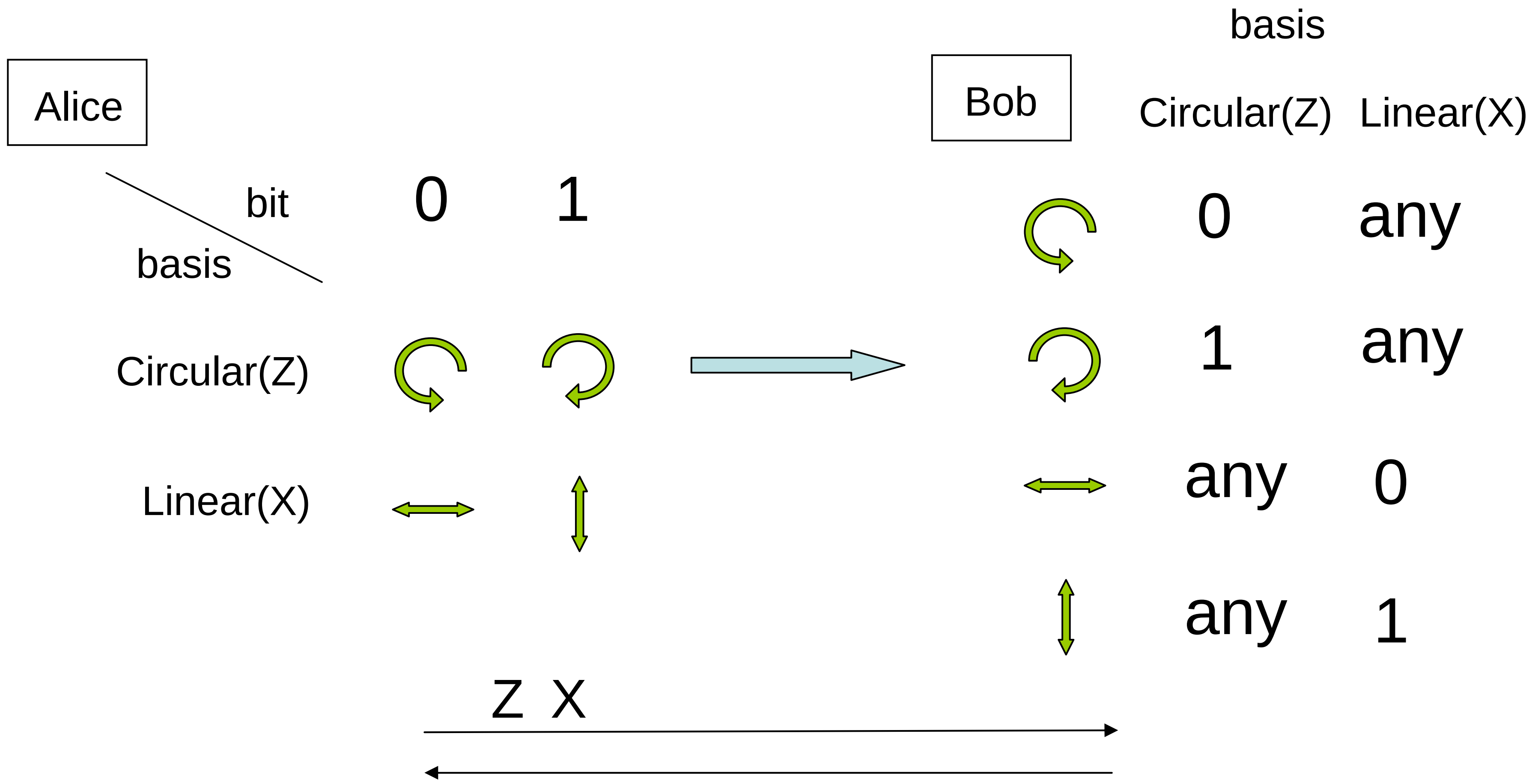
- Introduction
- Constraint on disturbance-free operations
  - Quantifying quantum information
- Monogamy of entanglement
  - Quantifying entanglement in unit of bits
- Unconditional security proofs
  - Difference between secret key and entanglement

Quantum key distribution (QKD)



BB84 protocol

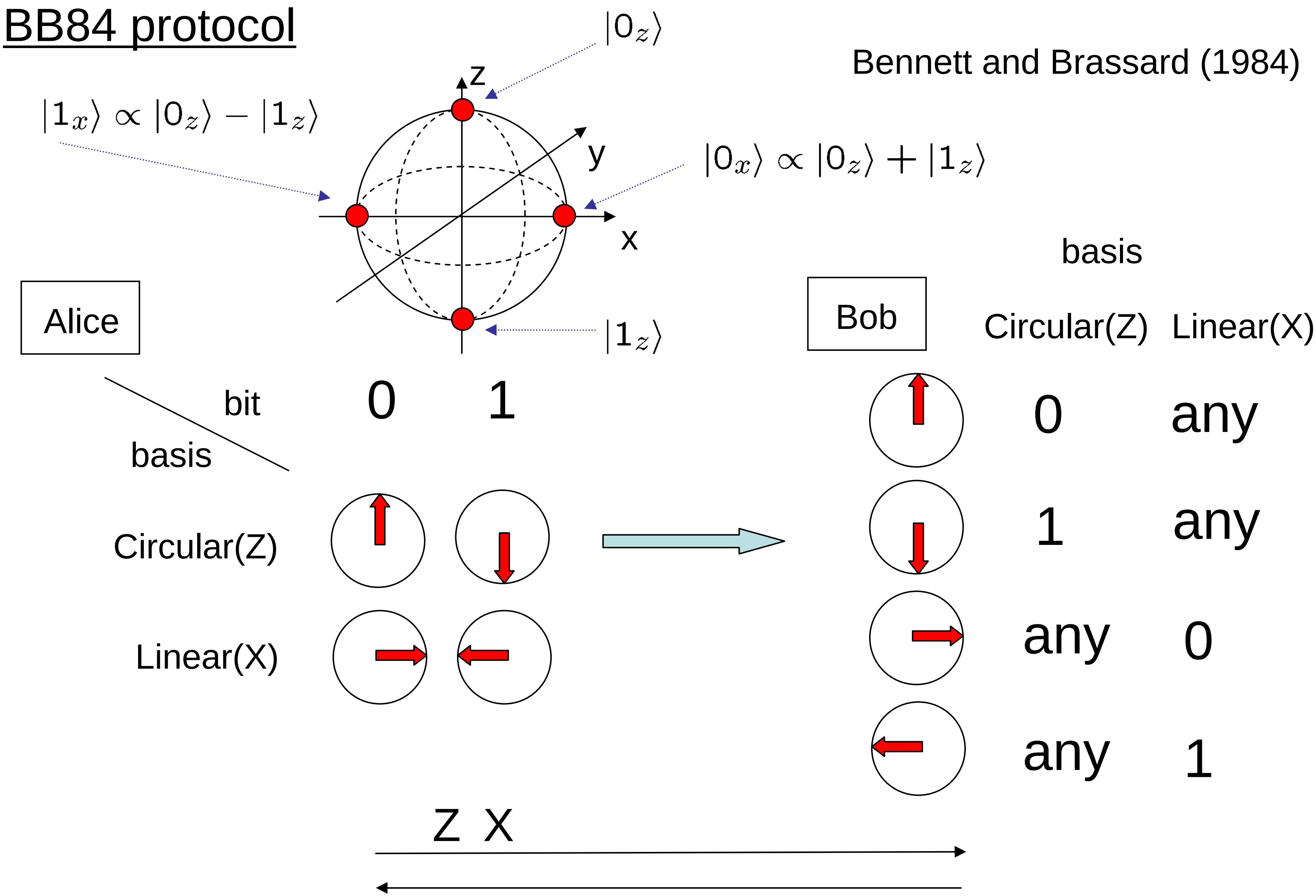
Bennett and Brassard (1984)



Discard if different bases are used (sifting).

BB84 protocol

Bennett and Brassard (1984)

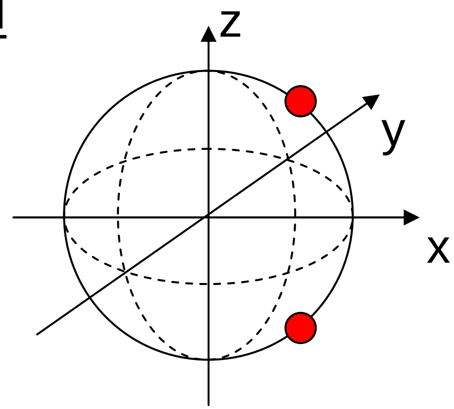


Discard if different bases are used (sifting).

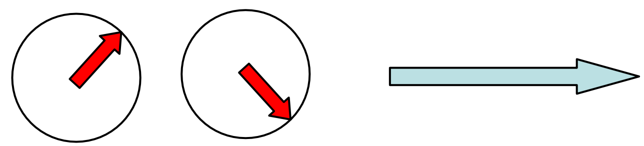
B92 protocol

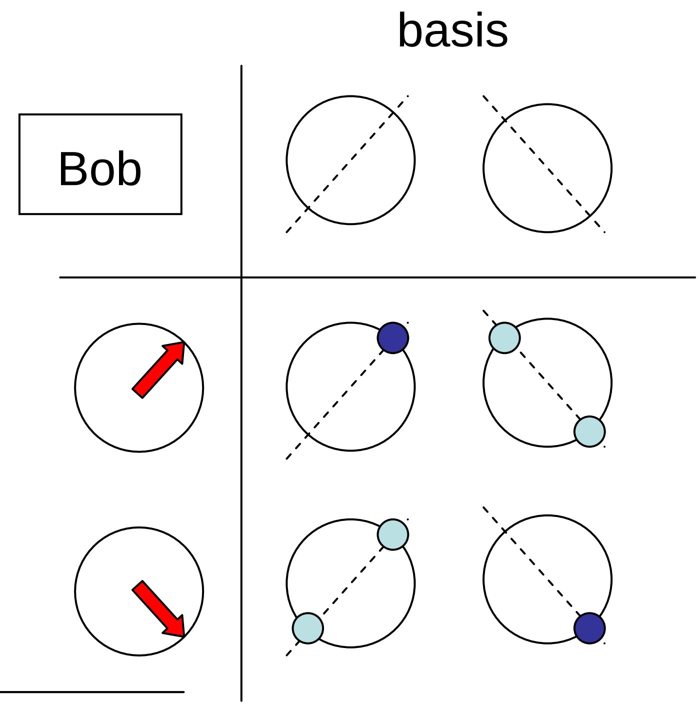
Bennett, PRL **68**, 3121 (1992).

Alice

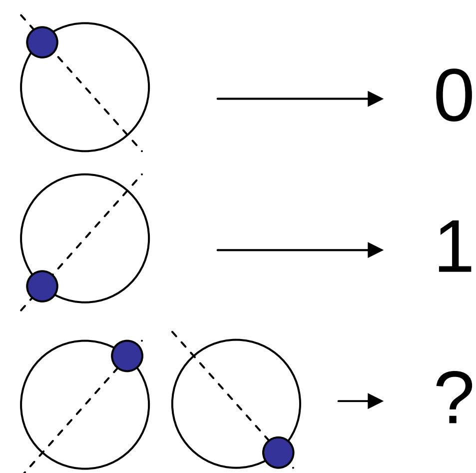


bit 0 1





Discard if the outcome is “?”

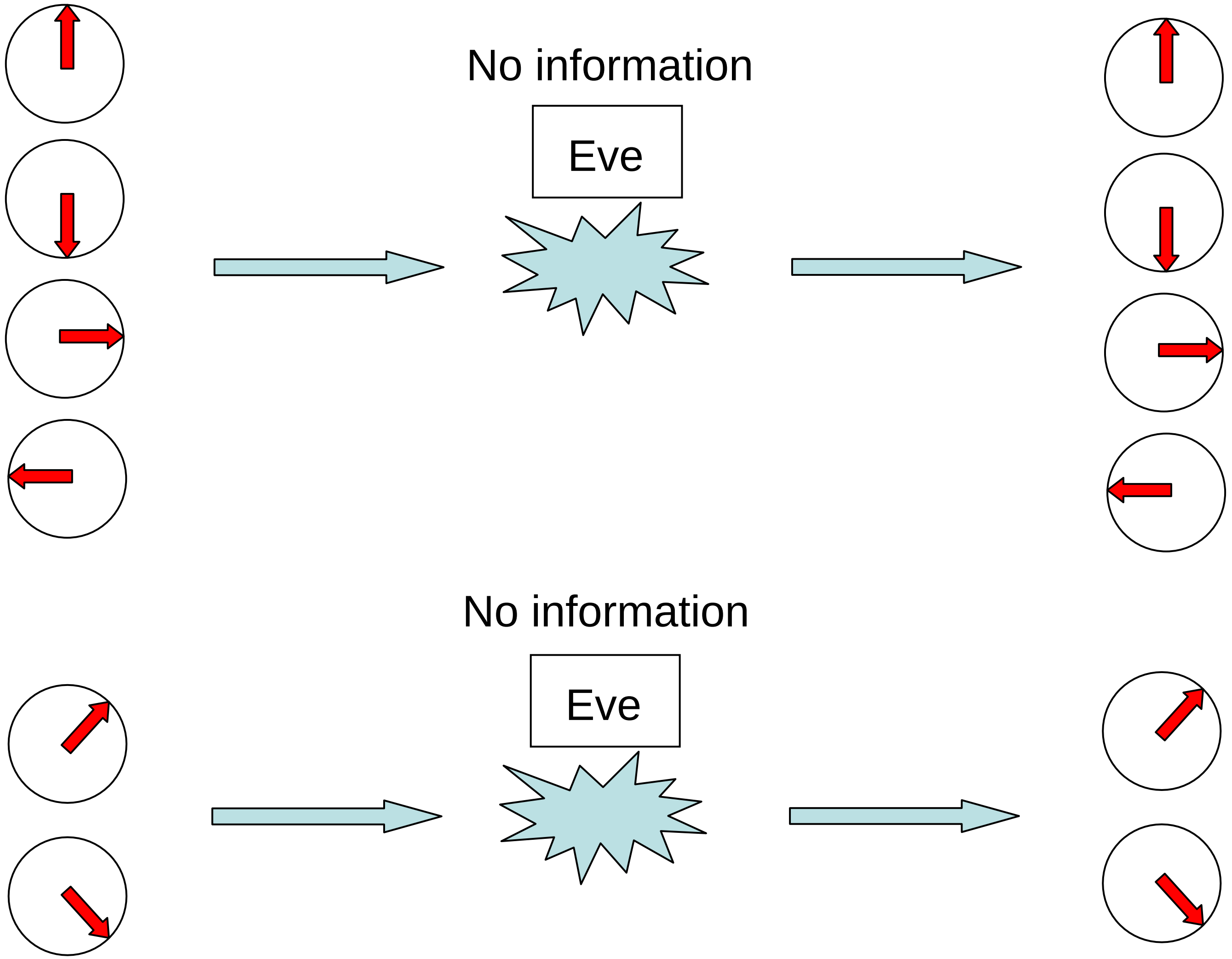


Any two nonorthogonal states can be used.

e.g. coherent states $|\alpha\rangle, |-\alpha\rangle$

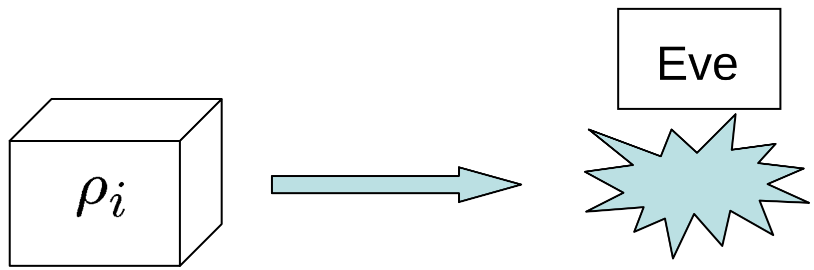
$$|\langle\alpha|-\alpha\rangle| = \exp(-2|\alpha|^2)$$

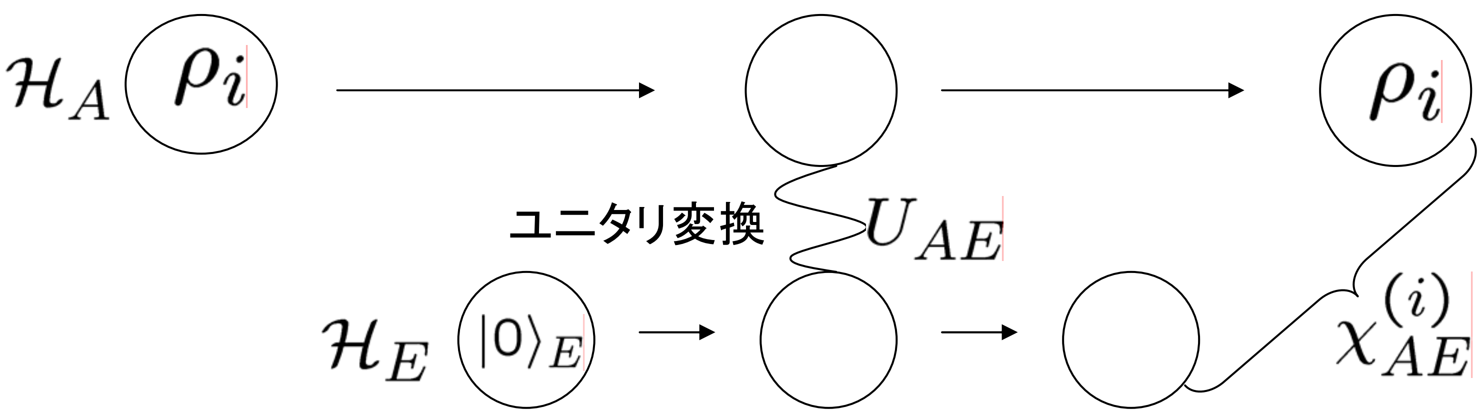
Zero-disturbance cases



Zero-disturbance cases (general input set)

$\{\rho_1, \rho_2, \cdots, \rho_i, \cdots\}$ Set of possible input states





$$\rho_i = \mathrm{Tr}_E[U_{AE}(\rho_i \otimes |0\rangle_E\langle 0|)U_{AE}^{\dagger}] \qquad \forall i$$

を満たすユニタリ演算子 U_{AE} とは何か？

Disturbance-free operations

Koashi & Imoto, PRL **81**,4264 (1998);
PRA **66**, 022318 (2002)

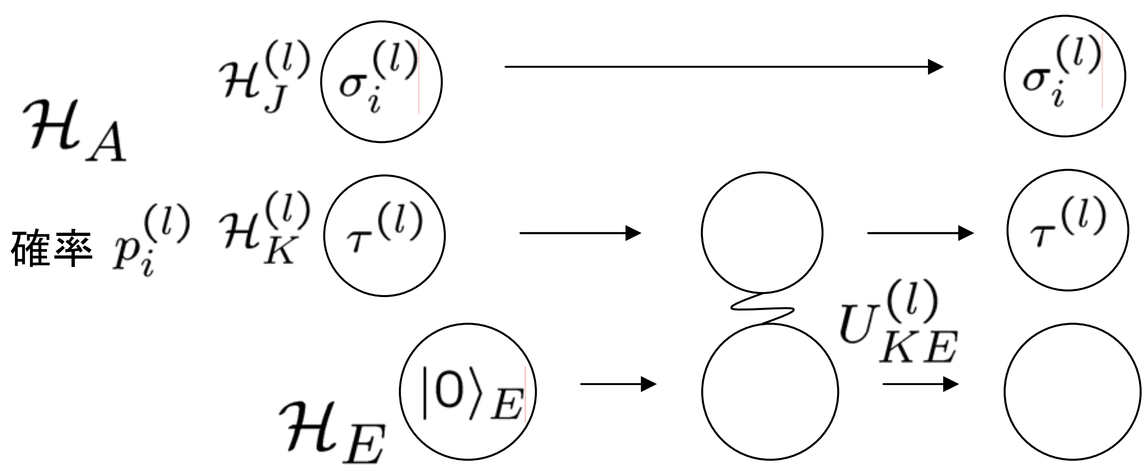
$\{\rho_1, \rho_2, \cdots, \rho_i, \cdots\}$ Set of possible input states

$$\rho_i = \mathrm{Tr}_E[U_{AE}(\rho_i \otimes |0\rangle_E\langle 0|)U_{AE}^\dagger] \quad \forall i$$

$$\{\rho_1, \rho_2, \ldots\} \xrightarrow{\text{unique}} \mathcal{H}_A = \bigoplus_l \mathcal{H}_J^{(l)} \otimes \mathcal{H}_K^{(l)}$$

$$\rho_i = \bigoplus_l p_i^{(l)} \sigma_i^{(l)} \otimes \tau^{(l)} \qquad U_{AE} = \bigoplus_l \mathbf{1}_J^{(l)} \otimes U_{KE}^{(l)}$$

$$\sum_l p_i^{(l)} = 1$$

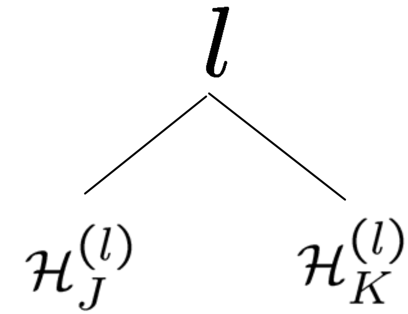


Summary of the theorem

自由度の分解

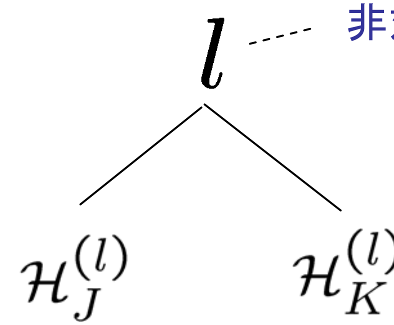
$$\mathcal{H}_A = \bigoplus_l \mathcal{H}_J^{(l)} \otimes \mathcal{H}_K^{(l)}$$

$$\dim \mathcal{H}_A = \sum_l (\dim \mathcal{H}_J^{(l)})(\dim \mathcal{H}_K^{(l)})$$



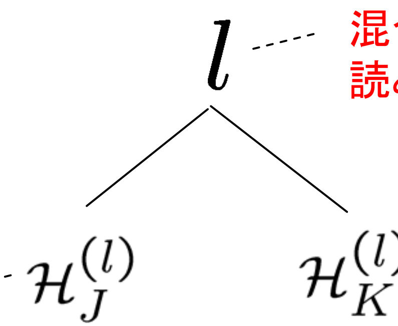
入力状態

$$\rho_i = \bigoplus_l p_i^{(l)} \sigma_i^{(l)} \otimes \tau^{(l)}$$



状態を変えない条件

$$U_{AE} = \bigoplus_l \mathbf{1}_J^{(l)} \otimes U_{KE}^{(l)}$$



盗聴者からビット値を守るには？

l

異なる値の状態間の混合は禁止（位相差は読み取れない）

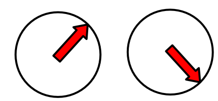
$\mathcal{H}_J^{(l)}$ 　　$\mathcal{H}_K^{(l)}$

全く触れない

Eveは $\mathcal{H}_J^{(l)}$ の中身を覗けない

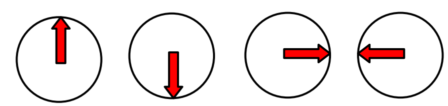
$\mathcal{H}_J^{(l)}$ にビット値を書き込む。

B92



$\mathcal{H}_J^{(l)}$ と、後から送る信号との古典相関にビット値を書き込む。

$\boxed{\text{基底の情報（X, Z）}}$



BB84

Eveは l の異なる値の部分空間にまたがった操作が出来ない。

物理量 l と、後から送る信号との量子相関にビット値を書き込む。

$$\frac{1}{\sqrt{2}}(|0\rangle_A|1\rangle_B+|1\rangle_A|0\rangle_B),\ \frac{1}{\sqrt{2}}(|0\rangle_A|1\rangle_B-|1\rangle_A|0\rangle_B),\ |0\rangle_A|0\rangle_B$$

Goldenberg & Vaidman, PRL **75**, 1239(1995)

$$\alpha|0\rangle_A|1\rangle_B+\beta|1\rangle_A|0\rangle_B,\ \beta^*|0\rangle_A|1\rangle_B-\alpha^*|1\rangle_A|0\rangle_B$$

Koashi & Imoto, PRL **79**, 2383(1997)

定量化の重要性

熱い、冷たい $\longrightarrow$ 温度 $\dashrightarrow$ 熱力学

情報が多い、少ない $\longrightarrow$ 情報量 $\dashrightarrow$ 情報科学

（bit）

量子系の状態の持つ情報量は？

qubit (＝光子1個の偏光状態)

「いろいろな量子状態が何qubit相当なのか？」

Quantifying information in a source

Quantifying the randomness of a probabilistic source

source → ABCDBCDBCABCDBC….

source → AAAAAABAAAAACA….

↓ Compression (coding)

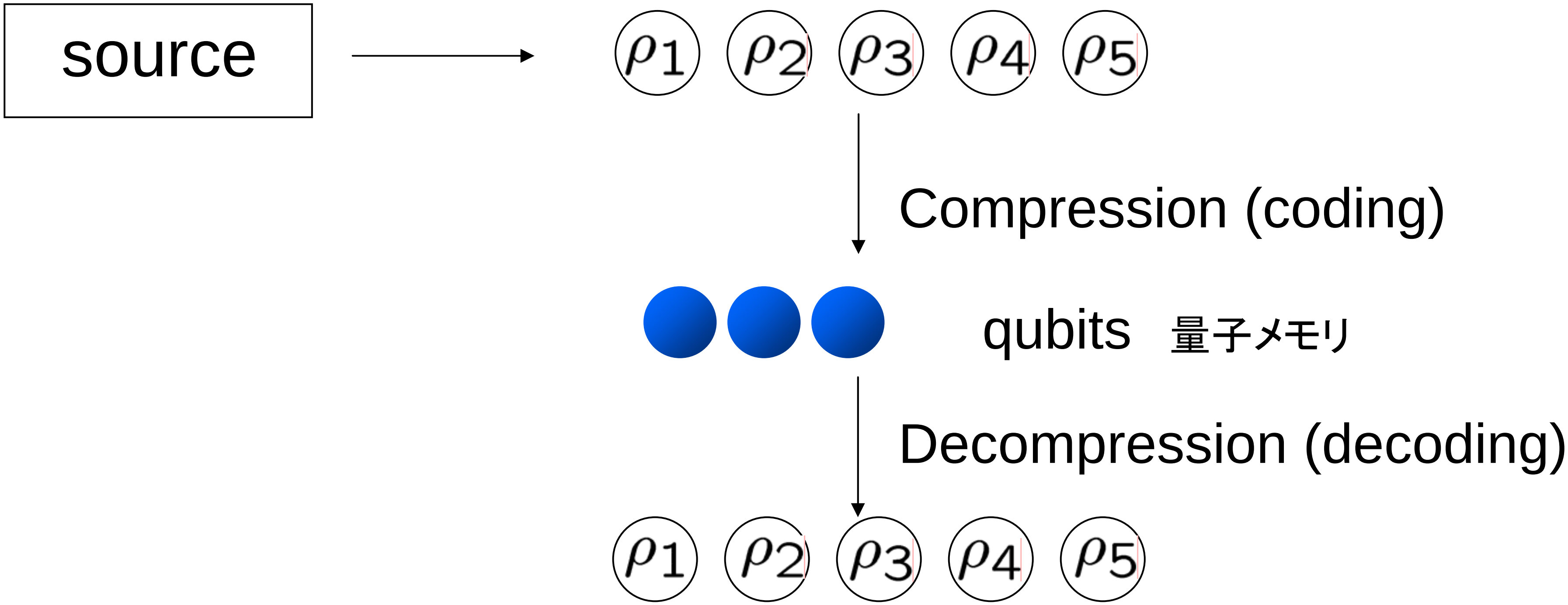
01001001...（古典）メモリ

↓ Decompression (decoding)

AAAAAABAAAAACA….

How many bits (per letter) are required to describe the sequence?

Quantifying information in a quantum source



How many qubits (per system) are required to reproduce the state?

情報の定量化～最適圧縮率

source

必要なメモリ

$$\{p_i, i\}$$

確率　古典的な「文字」

$$H(\{p_i\}) \equiv -\sum_i p_i \log_2 p_i$$ bits

Shannon(1948)

$$\{p_i, |i\rangle\}$$

確率　直交する純粋状態

$$H(\{p_i\}) \equiv -\sum_i p_i \log_2 p_i$$ bits

$$\{p_i, |i\rangle\}$$

確率　直交しない一般の純粋状態

$$\rho \equiv \sum_i p_i |i\rangle\langle i|$$

$$S(\rho) \equiv -\mathrm{Tr}[\rho \log_2 \rho]$$ qubits

Schumacher(1995)

情報の定量化～最適圧縮率

source

$\{p_i, i\}$

確率　　古典的な「文字」

必要なメモリ

$$H(\{p_i\}) \equiv -\sum_i p_i \log_2 p_i$$ bits

Shannon(1948)

$\{p_i, |i\rangle\}$

一般の純粋状態

$$\rho \equiv \sum_i p_i |i\rangle\langle i|$$

$$S(\rho) \equiv -\mathrm{Tr}[\rho \log_2 \rho]$$ qubits

Schumacher(1995)

$\{p_i, \rho_i\}$

一般の混合状態

$$\rho \equiv \sum_i p_i \rho_i$$

$$S(\rho) \equiv -\mathrm{Tr}[\rho \log_2 \rho]$$ qubits （十分）

まだ圧縮の余地が残る。

最適な圧縮率は？
どのくらい古典bitで代替できる？

一般の量子状態の最適圧縮率

Koashi & Imoto, PRL **87**,017902 (2001).

$$\{p_i, \rho_i\} \qquad \rho \equiv \sum_i p_i \rho_i$$

$$\{\rho_1, \rho_2, \ldots\} \longrightarrow \mathcal{H}_A = \bigoplus_l \mathcal{H}_J^{(l)} \otimes \mathcal{H}_K^{(l)}$$

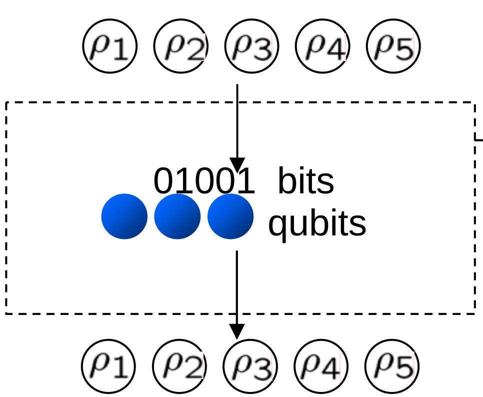
$$\rho_i = \bigoplus_l p_i^{(l)} \sigma_i^{(l)} \otimes \tau^{(l)}$$

$$\rho = \bigoplus_l p^{(l)} \sigma^{(l)} \otimes \tau^{(l)}$$

l は読み出しても状態は壊れない $\longrightarrow$ $H(\{p^{(l)}\})$ bits の古典メモリで十分

$\mathcal{H}_J^{(l)}$ の中身 $\longrightarrow$ $\sum_l p^{(l)} S(\sigma^{(l)})$ qubits の量子メモリで十分

$\mathcal{H}_K^{(l)}$ の中身 $\longrightarrow$ 保存の必要なし



$$U_{AE} = \bigoplus_l \mathbf{1}_J^{(l)} \otimes U_{KE}^{(l)}$$

制約

このblack boxから、

$H(\{p^{(l)}\})$ bits の古典メモリ

$\sum_l p^{(l)} S(\sigma^{(l)})$qubits の量子メモリ

を作ることができる。

$\longrightarrow$ これ以上の節約はできない

情報の定量化～最適圧縮率

source

必要なメモリ

$$\{p_i, i\}$$

確率　古典的な「文字」

$$H(\{p_i\}) \equiv -\sum_i p_i \log_2 p_i$$ bits

Shannon(1948)

$$\{p_i, |i\rangle\}$$

一般の純粋状態

$$\rho \equiv \sum_i p_i |i\rangle\langle i|$$

$$S(\rho) \equiv -\mathrm{Tr}[\rho \log_2 \rho]$$ qubits

Schumacher(1995)

$$\{p_i, \rho_i\}$$

一般の混合状態

$$\rho \equiv \sum_i p_i \rho_i = \bigoplus_l p^{(l)} \sigma^{(l)} \otimes \tau^{(l)}$$

$$H(\{p^{(l)}\})$$ bits

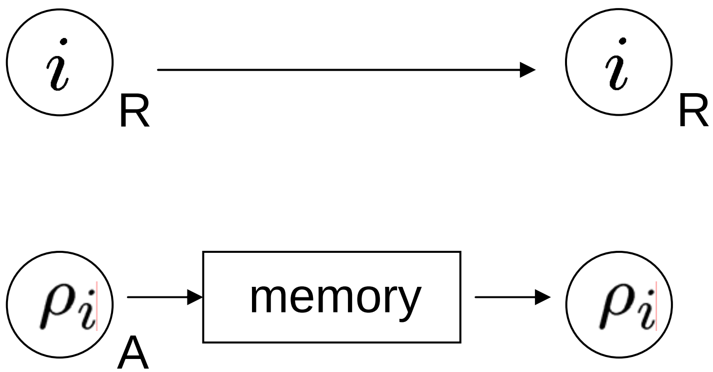
＋

$$\sum_l p^{(l)} S(\sigma^{(l)})$$ qubits

量子暗号の盗聴に対する安全性 $\longrightarrow$ 量子情報の定量化

情報の定量化～最適圧縮率

アンサンブル $\{p_i, \rho_i\}$ の保存



$$\chi_{RA} = \sum_i p_i |i\rangle\langle i| \otimes \rho_i$$

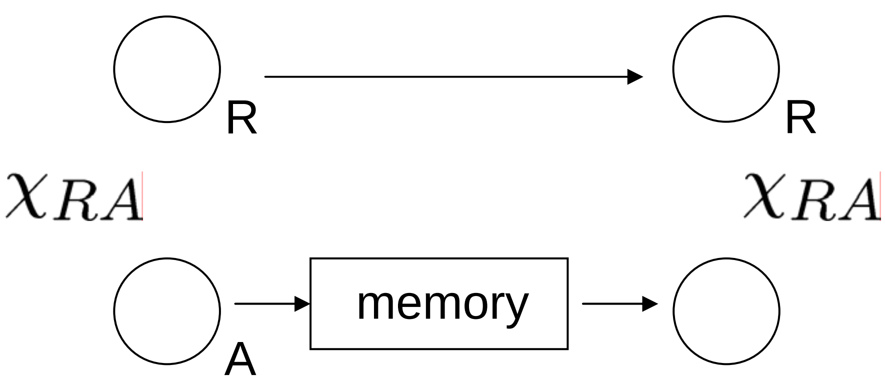
$$\rho \equiv \sum_i p_i \rho_i = \bigoplus_l p^{(l)} \sigma^{(l)} \otimes \tau^{(l)}$$

$H(\{p^{(l)}\})$ bits

+

$\sum_l p^{(l)} S(\sigma^{(l)})$ qubits

相関の保持（general bipartite states)



$$\chi_{RA} = \bigoplus_l p^{(l)} \xi_{RJ}^{(l)} \otimes \tau^{(l)}$$

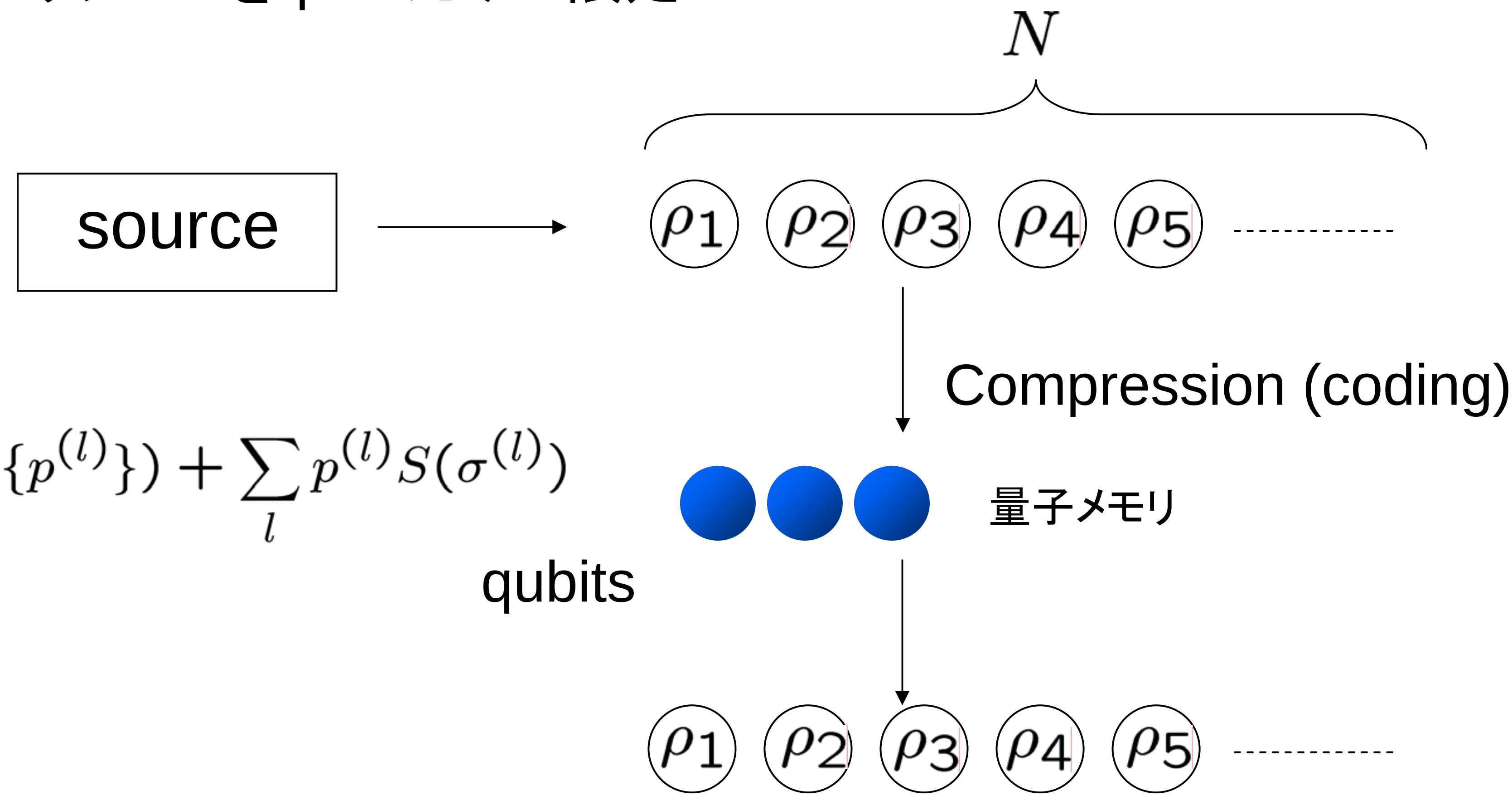
$$\sigma^{(l)} \equiv \mathrm{Tr}_R\, \xi_{RJ}^{(l)}$$

$H(\{p^{(l)}\})$ bits

+

$\sum_l p^{(l)} S(\sigma^{(l)})$ qubits

リソースをqubitだけに限定



$$H(\{p^{(l)}\}) + \sum_l p^{(l)} S(\sigma^{(l)})$$

今までの話の仮定

$$\text{Error} \to 0 \text{ for } N \to \infty$$

Asymptotically faithful

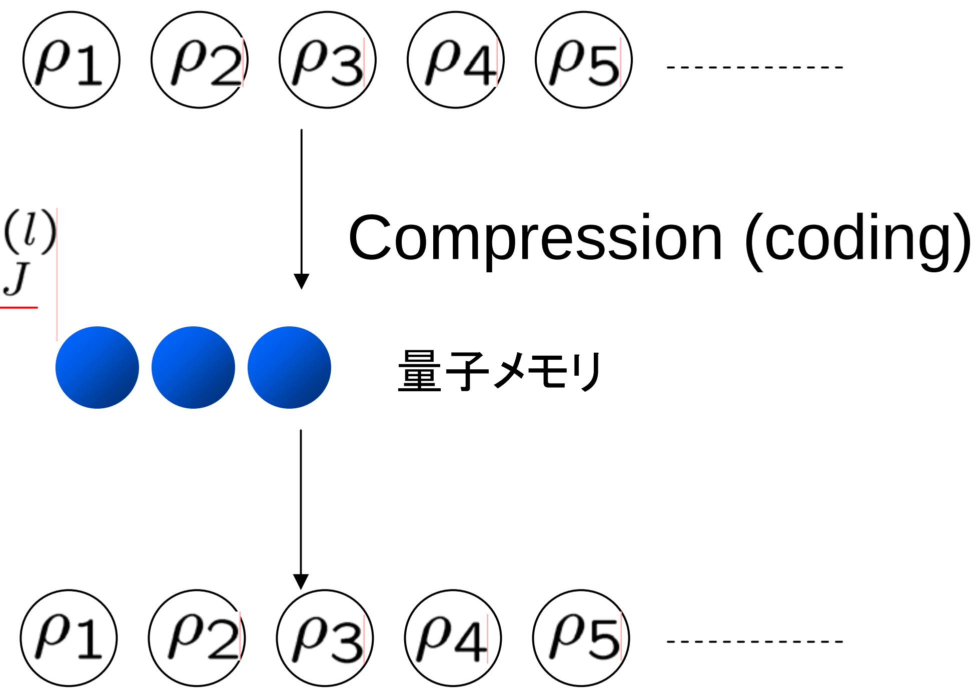
Zero error を要求したら？

Zero-error compression

Koashi & Imoto, PRL **89**, 097904 (2002).

必要なqubitの数は、入力に応じて変わってもよい。その期待値を
圧縮率と定義する。

source



$$H(\{p^{(l)}\}) + \sum_l p^{(l)} \underline{\log \dim \mathcal{H}_J^{(l)}}$$

qubits

$$\mathcal{H}_A = \bigoplus_l \mathcal{H}_J^{(l)} \otimes \mathcal{H}_K^{(l)}$$

$$\rho = \bigoplus_l p^{(l)} \sigma^{(l)} \otimes \tau^{(l)}$$

量子的な部分は、入力に応じて消費量を変える
ことができない（測定行為になってしまう）

リソースをqubitだけに限定

（問題設定自体には古典という概念は入っていない）

Asymptotically faithful

$$H(\{p^{(l)}\}) + \sum_l p^{(l)} S(\sigma^{(l)}) \quad \text{qubits}$$

Zero-error

$$H(\{p^{(l)}\}) + \sum_l p^{(l)} \log \dim \mathcal{H}_J^{(l)} \quad \text{qubits}$$

古典的な部分の圧縮率は条件によって変わらない

量子的な部分の圧縮率は条件によって変わる。

Entanglementの定量化

EPR qubit pair

リソース　　ebit　　$|\Phi^+\rangle \equiv \frac{1}{\sqrt{2}}(|0_z\rangle_A|0_z\rangle_B + |1_z\rangle_A|1_z\rangle_B)$

ρ_{AB} をLOCCで作り出すのに、何個のEPR qubit pairが必要か？

$\rho_{AB} = |\psi\rangle\langle\psi|$　なら、　$E(|\psi\rangle) \equiv S(\mathrm{Tr}_A|\psi\rangle\langle\psi|)$

一般には、

Entanglement cost

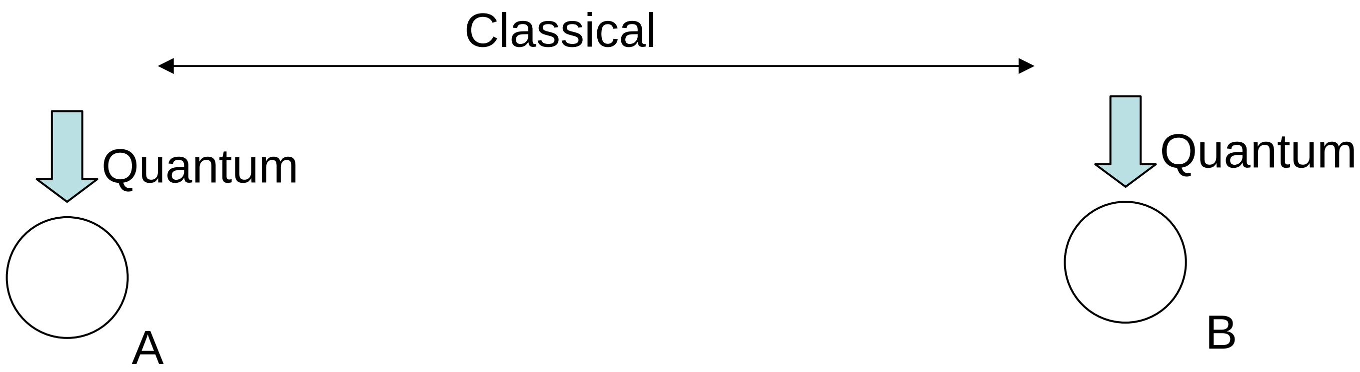
= Regularized entanglement of formation

$$E_C(\rho_{AB}) = \lim_{n\to\infty} \frac{1}{n} E_f(\rho_{AB}^{\otimes n})$$

$$E_f(\rho_{AB}) = \min_{\{p_i, |\psi_i\rangle\}} \sum_i p_i E\left(|\psi_i\rangle\right)$$

$$\sum_i p_i |\psi_i\rangle\langle\psi_i| = \rho_{AB}$$

<u>Local Operation and Classical Communication</u>



この制限の中でゼロから生成できる状態:　Separable states

$$\rho_{AB} = \sum_i p^{(j)} \rho_A^{(j)} \otimes \rho_B^{(j)}$$

それ以外の状態:　Entangled states

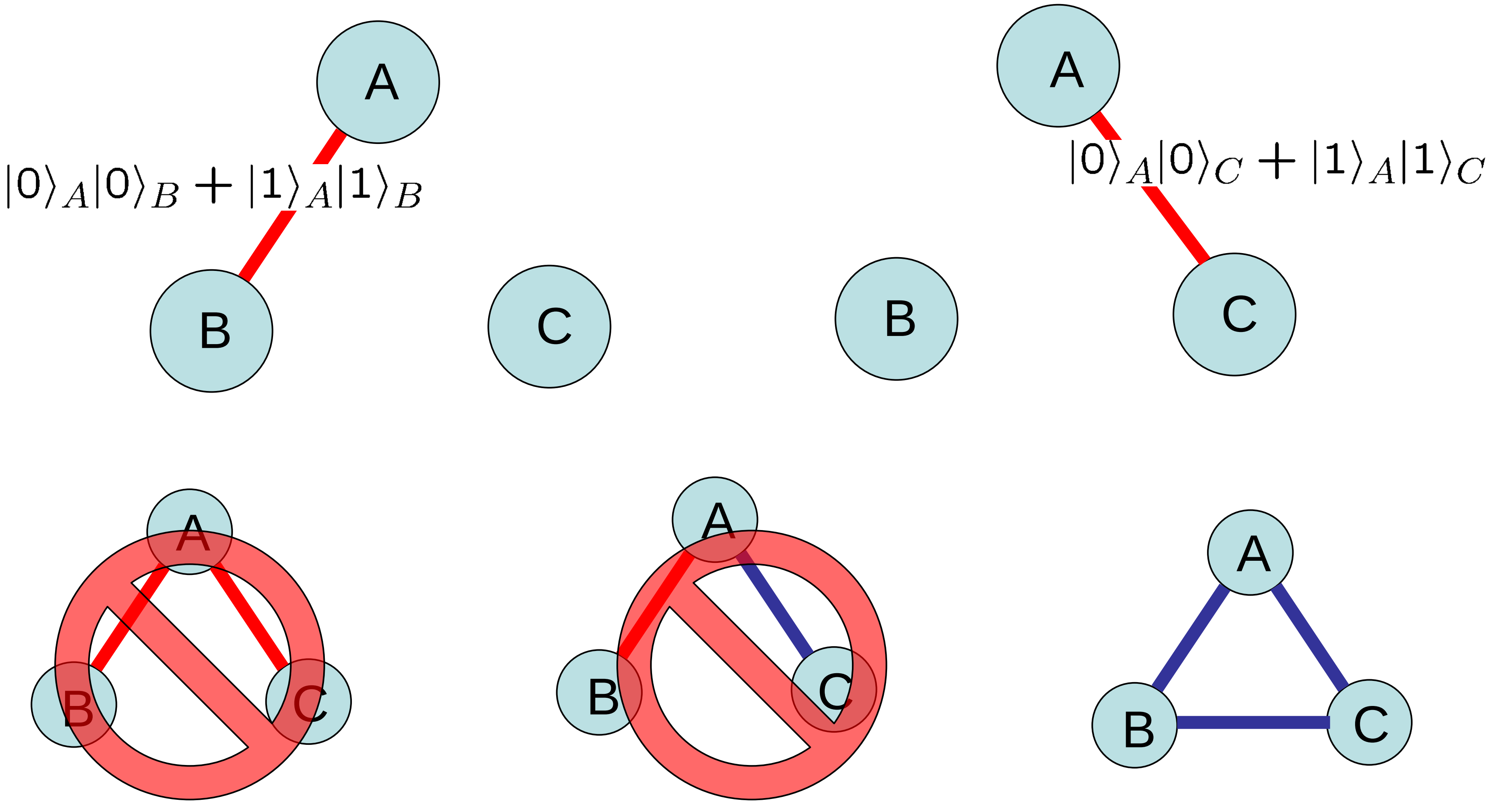
量子相関

ebit $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ entanglement

古典相関

rbit $\frac{1}{2}(|00\rangle\langle 00| + |11\rangle\langle 11|)$ common randomness

Monogamy of entanglement

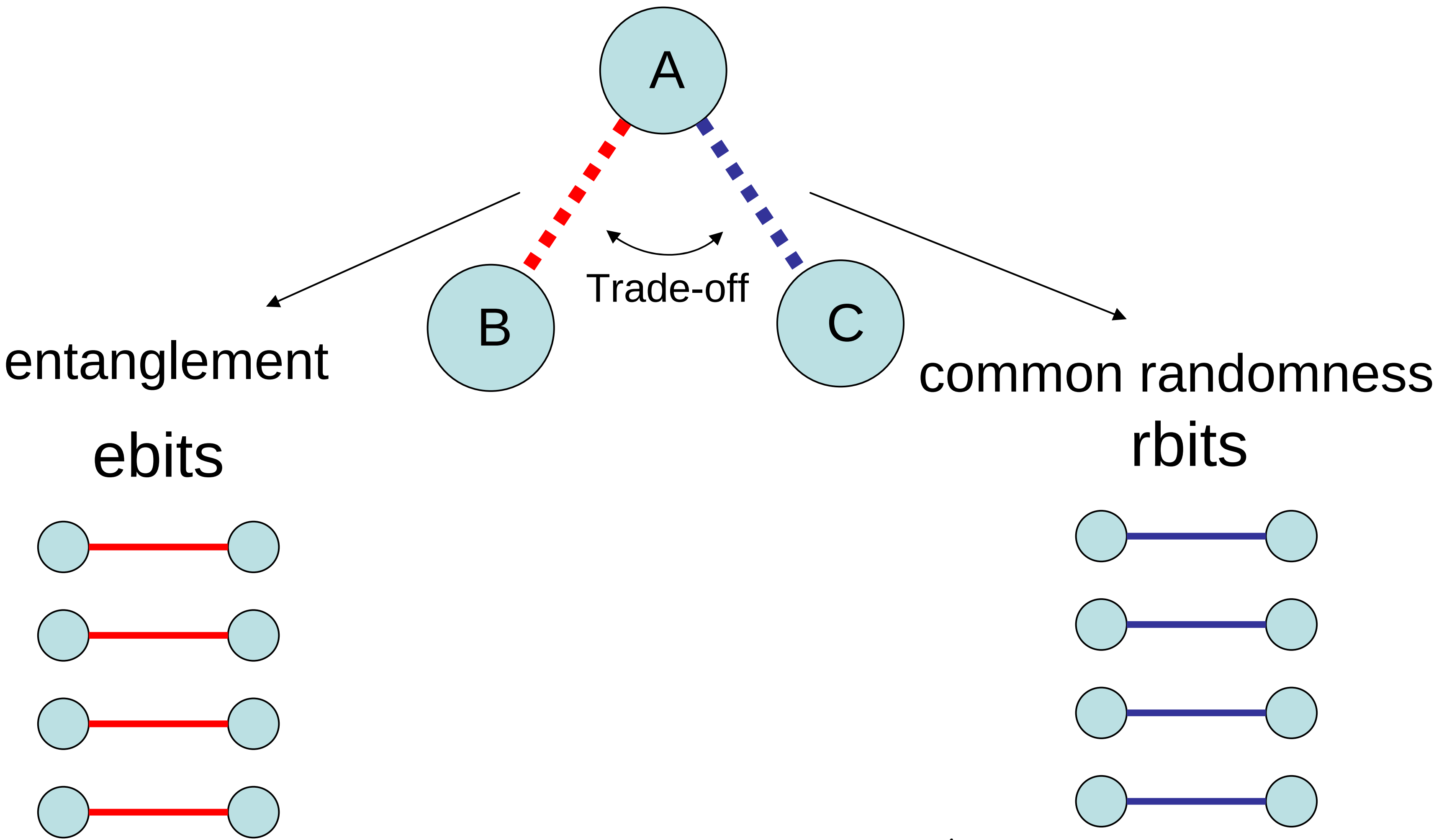


$$|0\rangle_A|0\rangle_B + |1\rangle_A|1\rangle_B$$

$$|0\rangle_A|0\rangle_C + |1\rangle_A|1\rangle_C$$

$$|000\rangle\langle 000| + |111\rangle\langle 111|$$

Quantum-classical trade-off

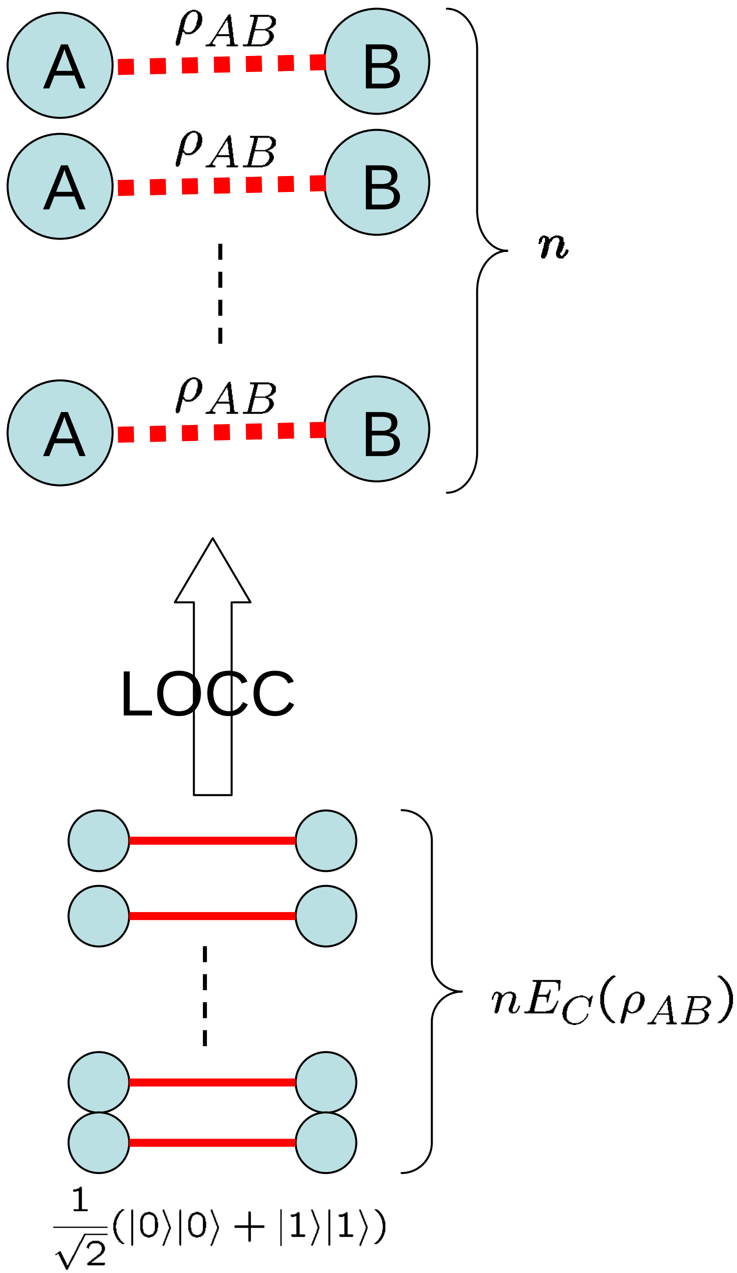


$$\frac{1}{\sqrt{2}}(|0\rangle|0\rangle + |1\rangle|1\rangle)$$

$$\frac{1}{2}(|00\rangle\langle 00| + |11\rangle\langle 11|)$$

Entanglement cost $E_C(\rho_{AB})$

Hayden, Horodecki, Terhal (2001)



Entanglement cost
= Regularized entanglement of formation

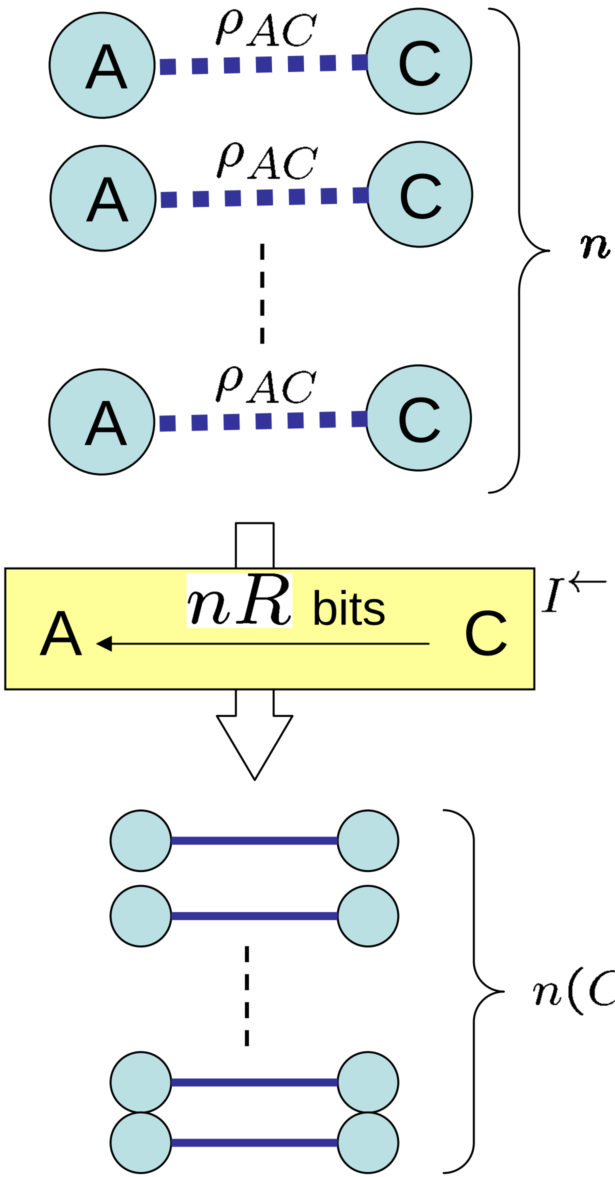
$$E_C(\rho_{AB}) = \lim_{n\to\infty} \frac{1}{n} E_f(\rho_{AB}^{\otimes n})$$

$$E_f(\rho_{AB}) = \min_{\{p_i, |\psi_i\rangle\}} \sum_i p_i E\left(|\psi_i\rangle\right)$$

$$\sum_i p_i |\psi_i\rangle\langle\psi_i| = \rho_{AB}$$

One-way distillable common randomness $C_D^{\leftarrow}(\rho_{AC})$

Devetak and Winter (2003)



$n(C_D^{\leftarrow}(\rho_{AC}) + R)$

$\frac{1}{2}(|00\rangle\langle 00| + |11\rangle\langle 11|)$

One-way distillable common randomness
= Regularized "Henderson-Vedral information"

$$C_D^{\leftarrow}(\rho_{AC}) = \lim_{n\to\infty} \frac{1}{n} I^{\leftarrow}(\rho_{AC}^{\otimes n})$$

$$I^{\leftarrow}(\rho_{AC}) = \max_{\{M_i\}} \chi(\{p_i, \rho_i\}) = \max_{\{M_i\}} [S(\rho_A) - \sum_i p_i S(\rho_i)]$$

$\{M_i\}$:POVM on C

$$p_i \equiv \mathrm{Tr}[(\mathbf{1}_A \otimes M_i)\rho_{AC}]$$

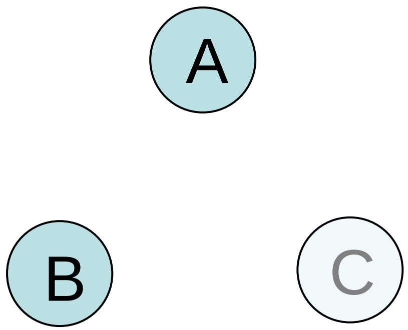
$$\rho_i \equiv \mathrm{Tr}_C[(\mathbf{1}_A \otimes M_i)\rho_{AC}]/p_i$$

$$\rho_A = \sum_i p_i \rho_i$$

Comparison of the two quantities

$$E_f(\rho_{AB}) = \min_{\{p_i, |\psi_i\rangle\}} \sum_i p_i E\left(|\psi_i\rangle\right) = \min_{\{p_i, |\psi_i\rangle\}} \sum_i p_i S\left(\rho_i\right)$$

$$\rho_i \equiv \mathrm{Tr}_B[|\psi_i\rangle\langle\psi_i|]$$



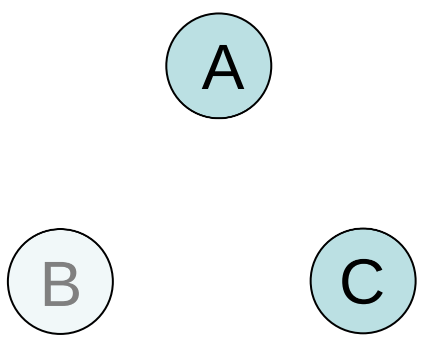
ensemble decomposition

$$\rho_{AB} \rightarrow \{p_i, |\psi_i\rangle\} \rightarrow \{p_i, \rho_i\}$$

discard system B

$$I^{\leftarrow}(\rho_{AC}) = \max_{\{M_i\}} \chi(\{p_i, \rho_i\}) = \max_{\{M_i\}}[S(\rho_A) - \sum_i p_i S(\rho_i)]$$

$$= S(\rho_A) - \min_{\{M_i\}}[\sum_i p_i S(\rho_i)]$$



Measurement on C

$$\rho_{AC} \rightarrow \{p_i, \rho_i\}$$

ρ_{ABC} が純粋状態なら、

ensemble decomposition of ρ_{AB}

||

Measurement on C

Monogamy relations

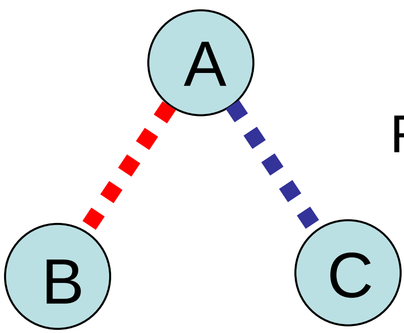
Koashi & Winter, Phys. Rev. A **69** 022309 (2004)

If ρ_{ABC} is pure,

$$E_f(\rho_{AB}) + I^{\leftarrow}(\rho_{AC}) = S(\rho_A)$$

$$E_C(\rho_{AB}) + C_D^{\leftarrow}(\rho_{AC}) = S(\rho_A)$$

Monogamy relations

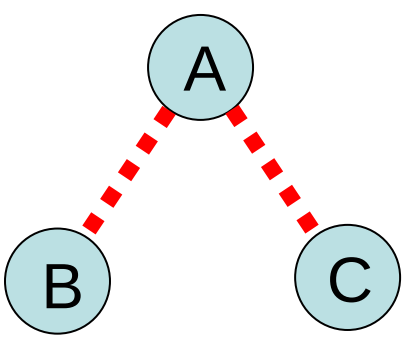


For any ρ_{ABC}

$$E_C(\rho_{AB}) + C_D^{\leftarrow}(\rho_{AC}) \leq S(\rho_A)$$

note

$$E_C(\rho_{AB}) + C_D^{\leftarrow}(\rho_{A(CD)}) = S(\rho_A)$$



$$E_C(\rho_{AB}) + E_D^{\leftarrow}(\rho_{AC}) \leq S(\rho_A)$$

note

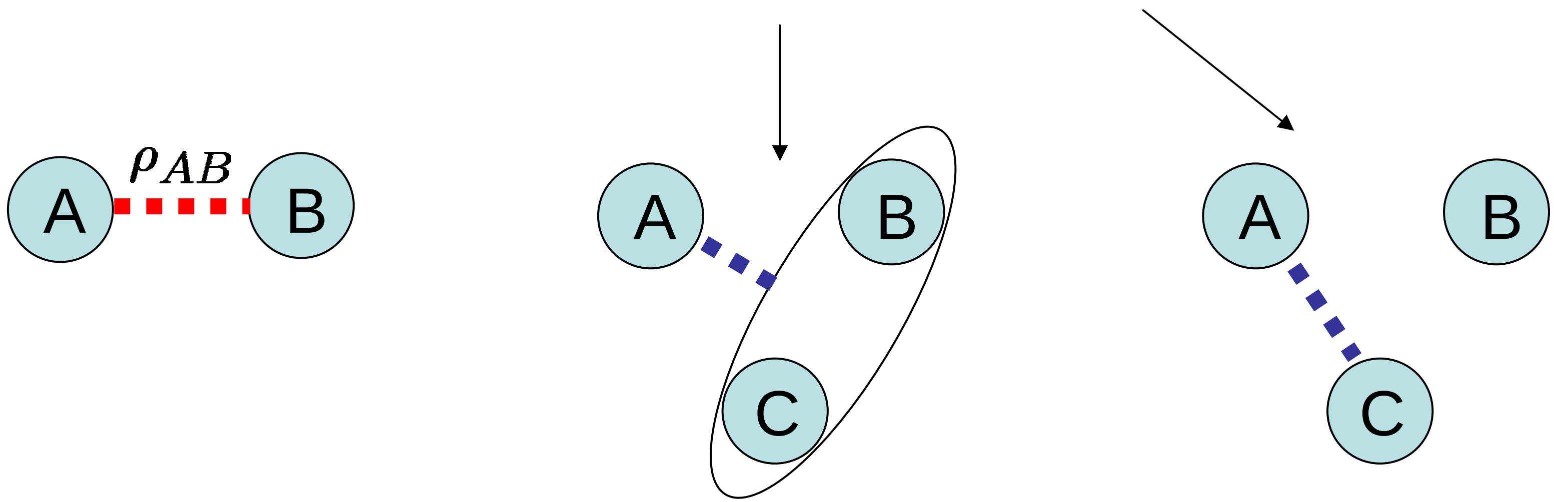
$$E_D^{\leftarrow}(\rho_{AC}) \leq C_D^{\leftarrow}(\rho_{AC})$$

A measure of entanglement in unit of bits

If ρ_{ABC} is pure,

$$E_C(\rho_{AB}) + C_D^{\leftarrow}(\rho_{AC}) = S(\rho_A) = C_D^{\leftarrow}(\rho_{A(BC)})$$

$$E_C(\rho_{AB}) = C_D^{\leftarrow}(\rho_{A(BC)}) - C_D^{\leftarrow}(\rho_{AC})$$



Distillable common randomness with the help of B

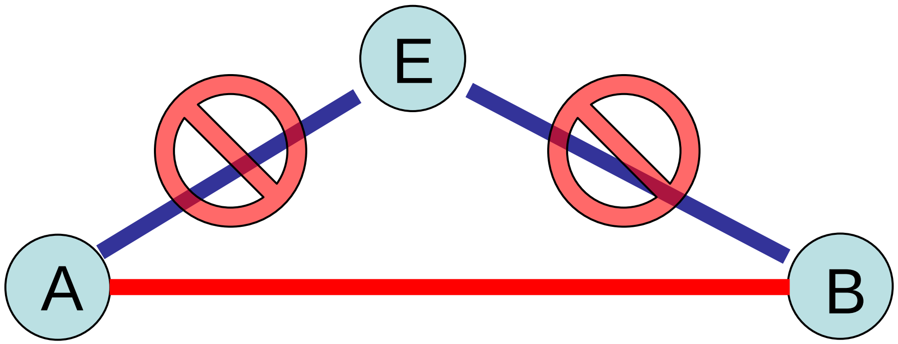
Distillable common randomness without B

This definition gives a measure equal to $E_C(\rho_{AB})$, but its unit is “rbit”.

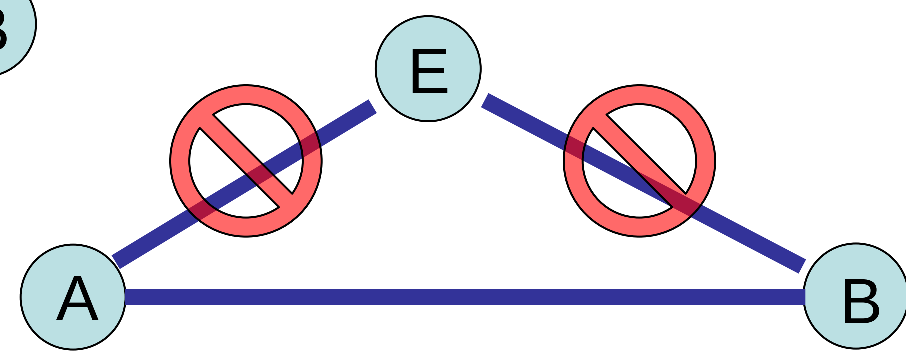
The monogamy property can be a defining property of entanglement.

Monogamy of entanglement and quantum key distribution

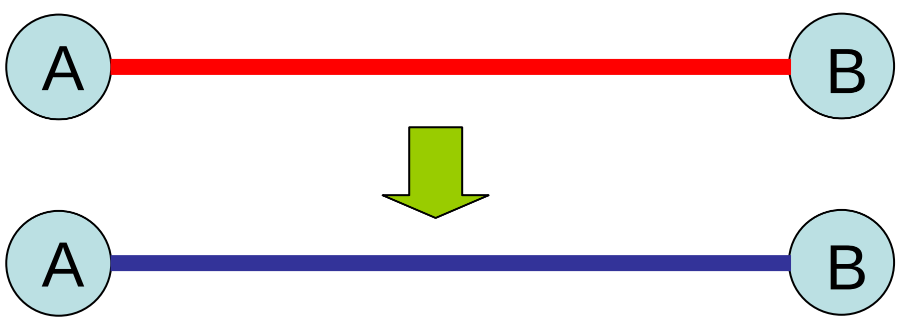
Monogamy



Secret key



Quantum correlation > classical correlation

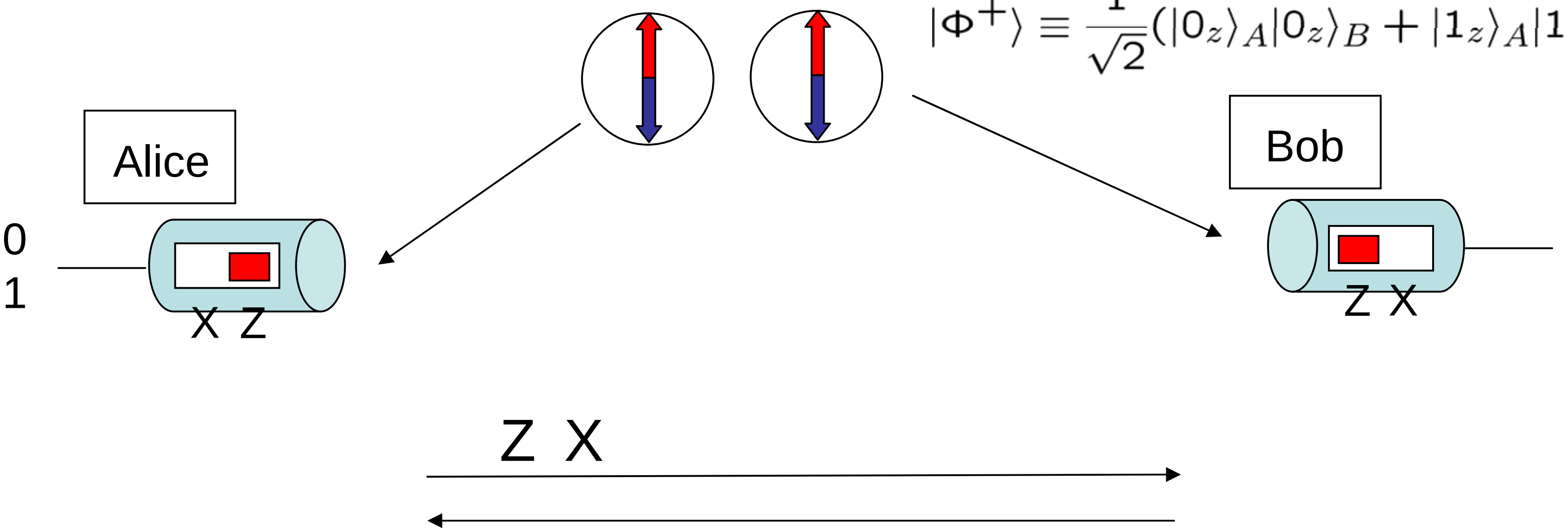


Ekert (E91, BBM92) protocol

Ekert, PRL **67**, 661 (1991);
Bennett, Brassard, Mermin, PRL **68**,557 (1992).

MES(Maximally entangled state)

$$|\Phi^+\rangle \equiv \frac{1}{\sqrt{2}}(|0_z\rangle_A|0_z\rangle_B + |1_z\rangle_A|1_z\rangle_B)$$

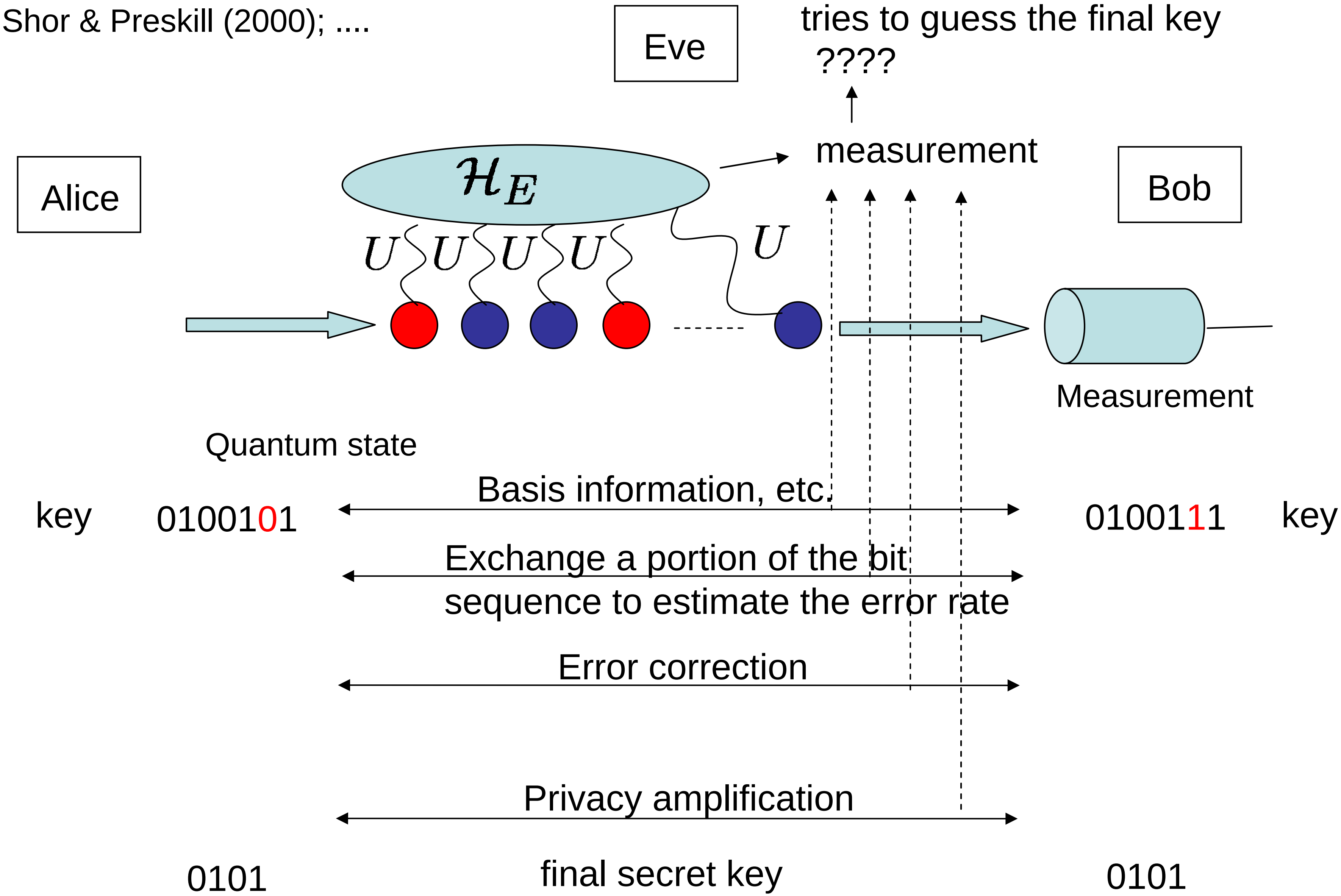


Discard if different bases are used (sifting).

$$|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|0_z\rangle_A|0_z\rangle_B+|1_z\rangle_A|1_z\rangle_B) = \frac{1}{\sqrt{2}}(|0_x\rangle_A|0_x\rangle_B+|1_x\rangle_A|1_x\rangle_B)$$

Unconditional security: Against coherent attacks

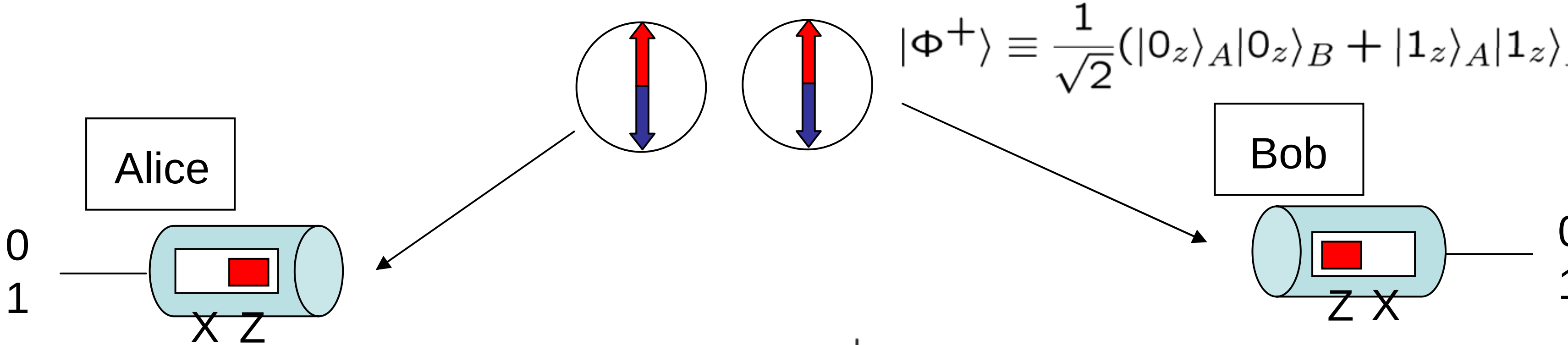
Mayers (1996); Lo & Chau (1999);
Shor & Preskill (2000); ....



Security of Ekert protocol

MES(Maximally entangled state)

$$|\Phi^+\rangle \equiv \frac{1}{\sqrt{2}}(|0_z\rangle_A|0_z\rangle_B + |1_z\rangle_A|1_z\rangle_B)$$



If they do share the state $|\Phi^+\rangle$

1) The obtained pair of bits are perfectly correlated and random.
2) Eve has no clue on the bit value.

"No one can predict the outcome of a measurement on a pure state."

It suffices to make sure that the state <u>in Alice's and Bob's hands</u> is

$$|\Phi^+\rangle \equiv \frac{1}{\sqrt{2}}(|0_z\rangle_A|0_z\rangle_B + |1_z\rangle_A|1_z\rangle_B)$$

No need to guess what state Eve may have.

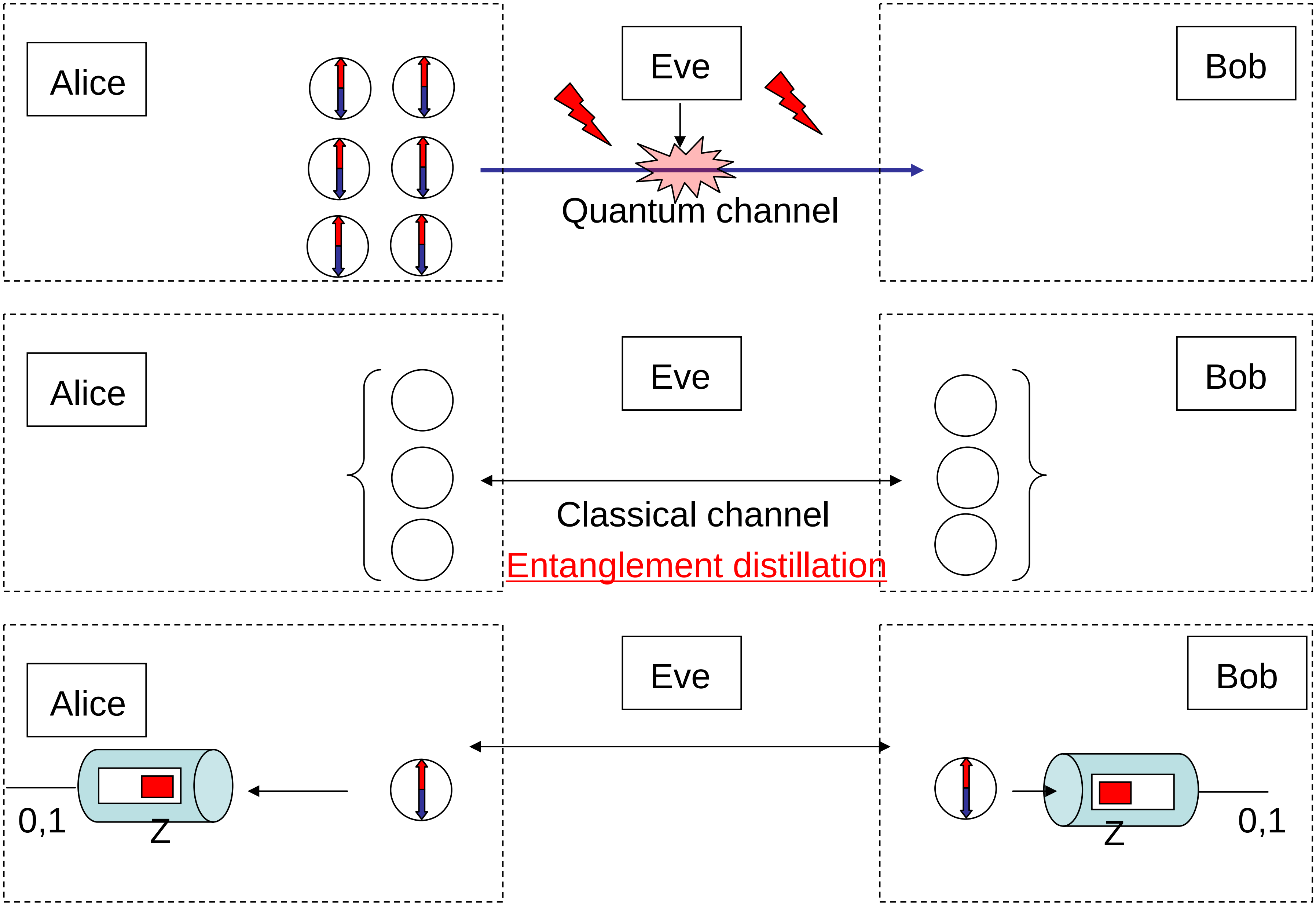
How can we share MES under noises or intervention by Eve?

→ Entanglement distillation

Bennett, Brassard, Popescu, Schumacher, Smolin, Wootters (1996)

Entanglement distillation and QKD

Deutsch, Ekert, Jozsa, Macchiavello, Popescu, Sanpera (1996).
Lo, Chau (1999).



Unconditional security proofs based on entanglement distillation

Ekert protocol

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

BB84 protocol

CSS quantum error correcting code
Classical probability estimate

Shor & Preskill, Phys. Rev. Lett. **85**, 441 (2000).

B92 protocol

Local filtering
Nonorthogonal probability estimate

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

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

Distillable entanglement $E_D(\rho_{AB})$ (ebits)

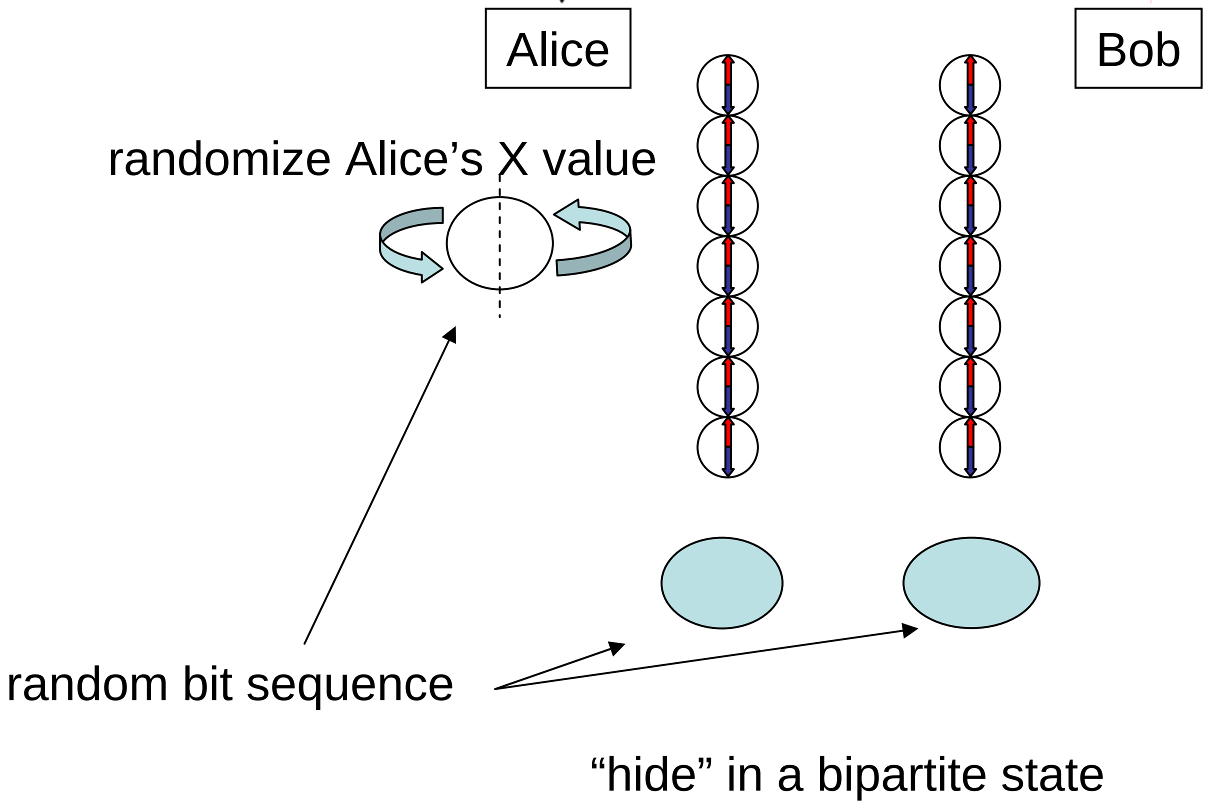
Distillable secret key $C_{\text{secret}}(\rho_{AB})$ (bits)

$$E_D(\rho_{AB}) \overset{?}{=} C_{\text{secret}}(\rho_{AB})$$

Secret key vs. distillable entanglement

Horodecki's & Oppenheim,
Phys. Rev. Lett. **94**, 160502 (2005).

$$|\Phi^+\rangle \equiv \frac{1}{\sqrt{2}}(|0_z\rangle_A|0_z\rangle_B + |1_z\rangle_A|1_z\rangle_B)$$



Alice cannot recover the X value by LOCC with Bob.

$\longrightarrow$ distillable entanglement は減る。

Distillable secret keyは変わらず。

$$E_D(\rho_{AB}) < C_{\text{secret}}(\rho_{AB})$$

$E_D(\rho_{AB}) < C_{\mathrm{secret}}(\rho_{AB})$ となる例が存在

EPR対を取り出すよりもsecret keyを取り出すほうが簡単

Separable (no entanglement)

$$\rho_{AB} = \sum_i p^{(j)} \rho_A^{(j)} \otimes \rho_B^{(j)}$$

$$\rho_{ABE} = \sum_i p^{(j)} \rho_A^{(j)} \otimes \rho_B^{(j)} \otimes |j\rangle_E\langle j|$$

Eveから見て、AliceとBobは相関なし

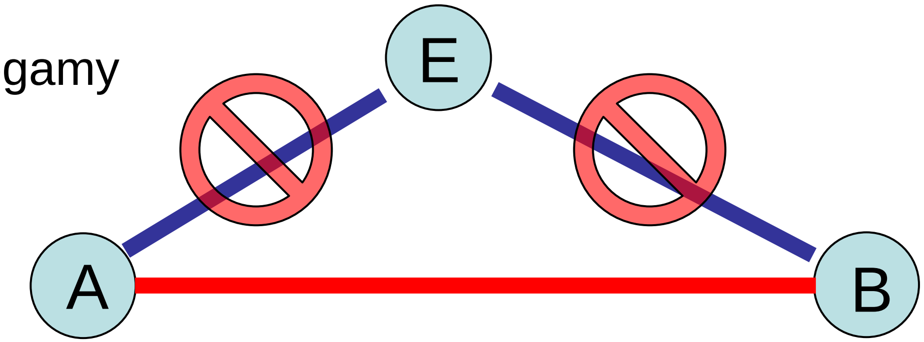
$\longrightarrow$ No secret key

Secret keyを取り出すにはentanglementが必要

entanglementのどんな性質が重要なのか？

EPR対からsecret keyが作れる理由

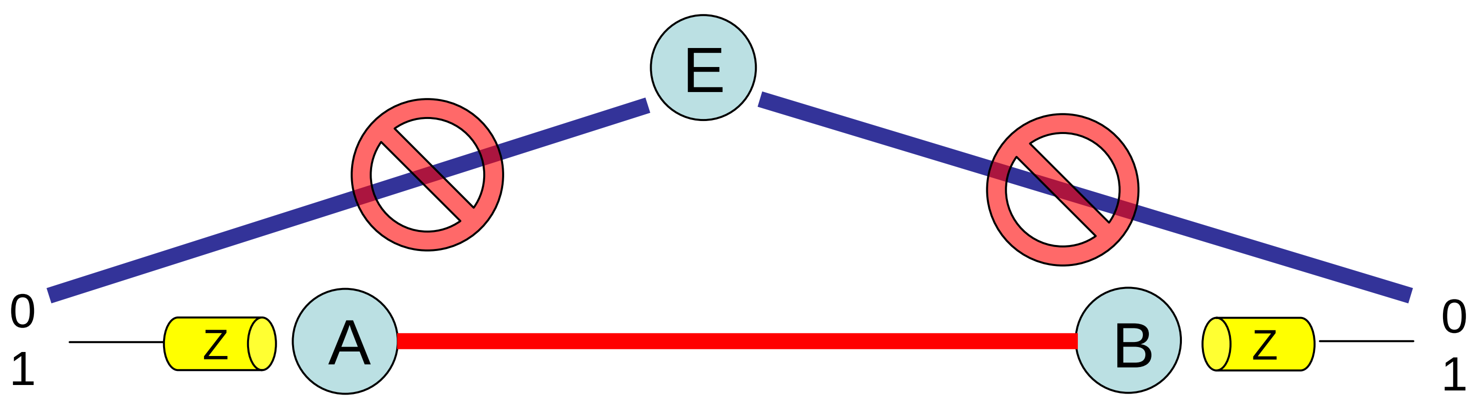
Monogamy



$$|\Phi^+\rangle \equiv \frac{1}{\sqrt{2}}(|0_z\rangle_A|0_z\rangle_B + |1_z\rangle_A|1_z\rangle_B)$$

- 純粋状態

- Z基底で完全相関



EPR対からsecret keyが作れる理由

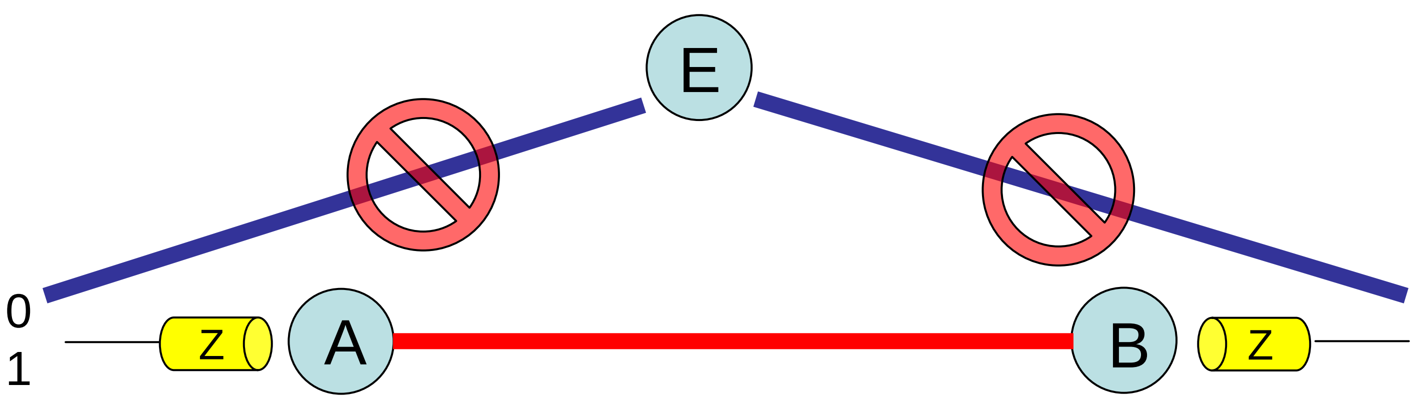
$$|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|0_z\rangle_A|0_z\rangle_B+|1_z\rangle_A|1_z\rangle_B) = \frac{1}{\sqrt{2}}(|0_x\rangle_A|0_x\rangle_B+|1_x\rangle_A|1_x\rangle_B)$$

- X基底で完全相関 → Aliceはqubit BのX基底の結果を予言できる。

“不確定性関係”(Robertson type)

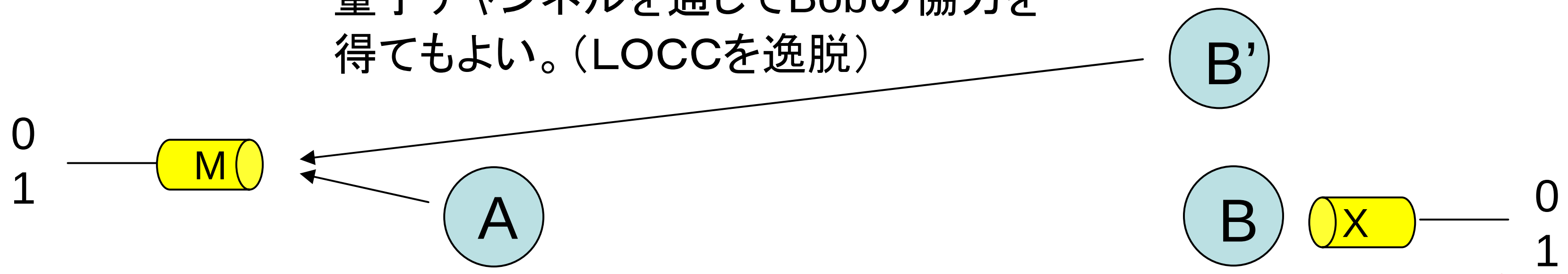
- Z基底で完全相関

Eveはqubit BのZ基底の結果を予言できない。



EPR対からsecret keyが作れる理由

量子チャンネルを通してBobの協力を
得てもよい。（LOCCを逸脱）



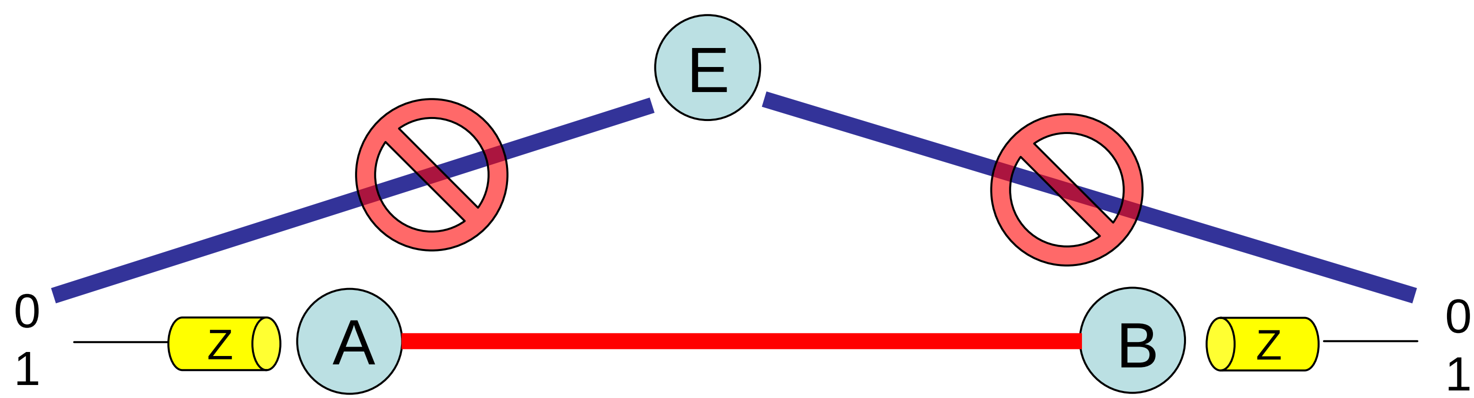
$$|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|0_z\rangle_A|0_z\rangle_B+|1_z\rangle_A|1_z\rangle_B) = \frac{1}{\sqrt{2}}(|0_x\rangle_A|0_x\rangle_B+|1_x\rangle_A|1_x\rangle_B)$$

- Eveとqubit B以外の系を使ってqubit BのX基底の結果を予言できる。

“不確定性関係”(Robertson type)

- Z基底で完全相関

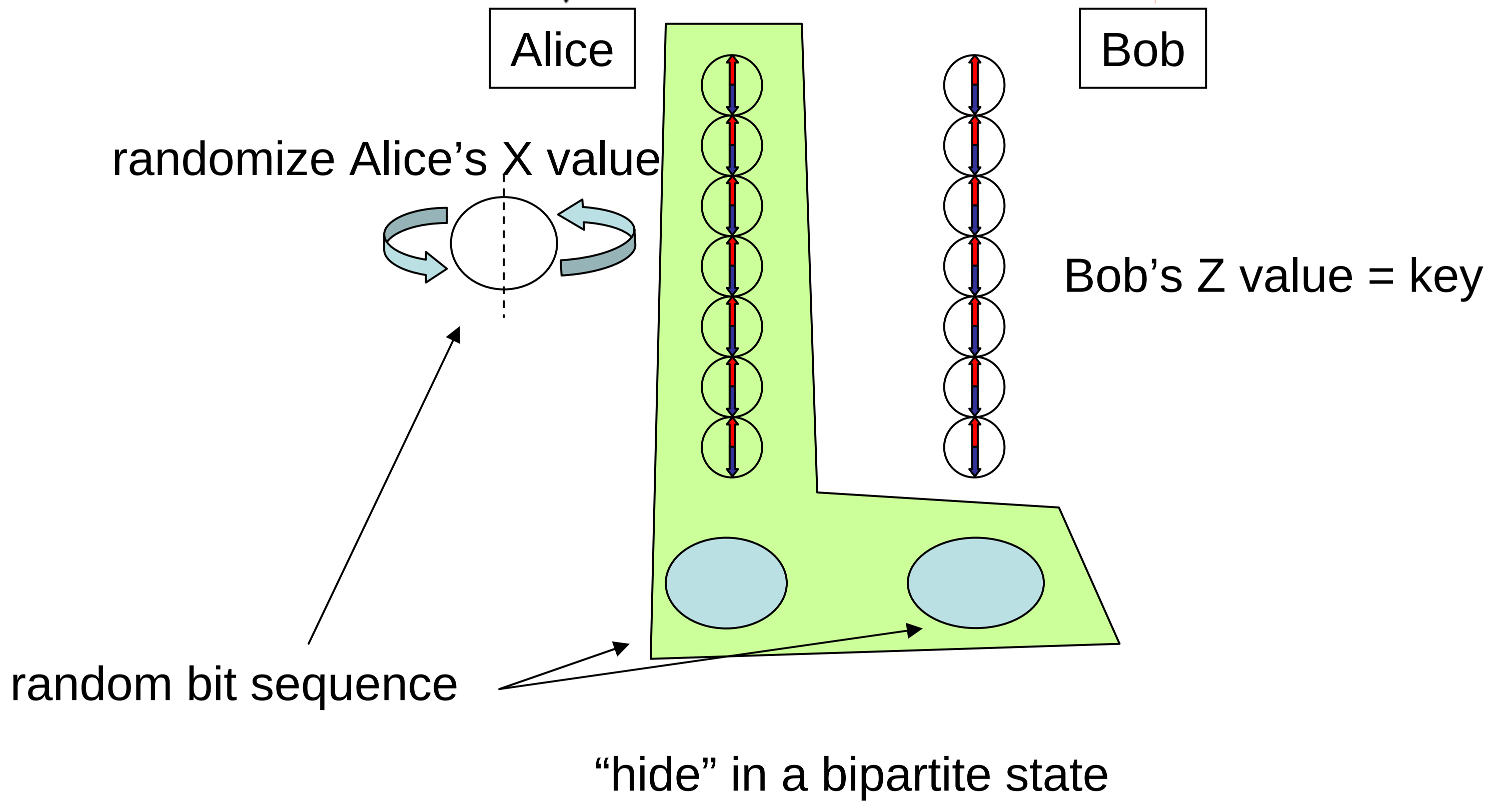
Eveはqubit BのZ基底の結果を予言できない。



Secret key vs. distillable entanglement

Horodecki's & Oppenheim,
Phys. Rev. Lett. **94**, 160502 (2005).

$$|\Phi^+\rangle \equiv \frac{1}{\sqrt{2}}(|0_z\rangle_A|0_z\rangle_B + |1_z\rangle_A|1_z\rangle_B)$$



Alice cannot recover the X value by LOCC with Bob.

$\longrightarrow$ distillable entanglement は減る。

$$E_D(\rho_{AB}) < C_{\text{secret}}(\rho_{AB})$$

Distillable secret keyは変わらず。

Unconditional security proof based on uncertainty principle

- Enjoys the versatility of Shor-Preskill argument

- By encrypting the error correction step, we can decouple it from the privacy amplification.

  Any error correction method + random parity

- Uncharacterized apparatuses

  ex) BB84 with arbitrary source for which only the basis-dependence is known

- Possible to have a key rate strictly larger than the distillable entanglement

Koashi & Preskil, Phys. Rev. Lett. **90**, 057902 (2003);
Koashi, quant-ph/0505108.

まとめ

量子暗号 ---------------------- 量子系の基本的な性質と密接な関係

測定と反作用
応用上の要請に基づく定量的な議論

反作用ゼロのケース → 量子情報の定量化

古典メモリ、量子メモリ

一般に反作用による
エラーがある場合

Monogamy of entanglement
による安全性証明 → entanglementの古典相関
(bit)による定量化

不確定性関係による
安全性証明 → secret key とentanglementの関係

単位となるリソースを指定して
部分系間の相関を定量化

そのリソースの持つ意味は？