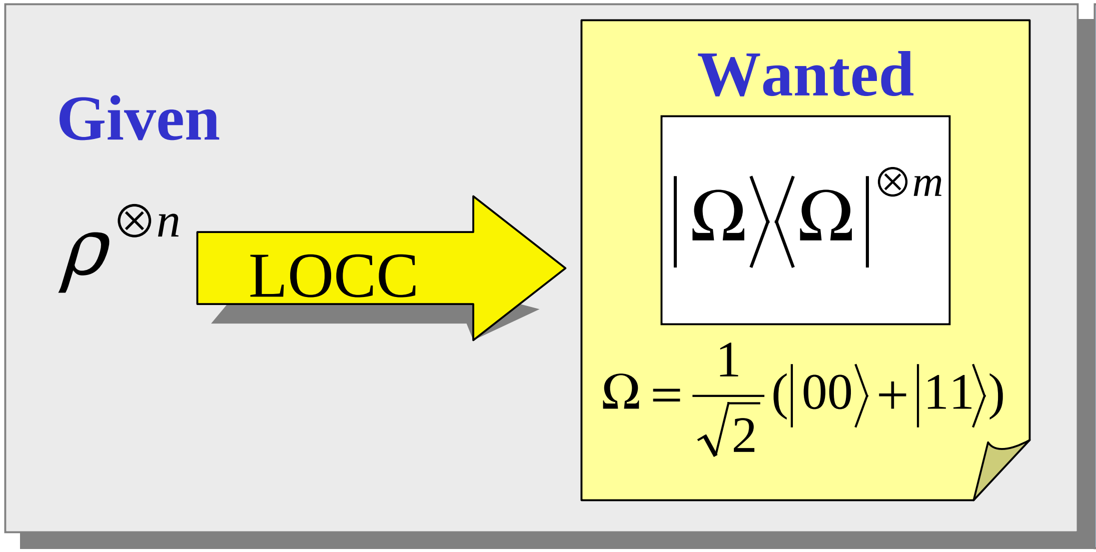
Distillation beyond qubits

„Efficient Distillation beyond qubits“ (*Vollbrecht*, *Wolf*) quant-ph/0208152

„On the Irreversibility of Entanglement Distillation“ (*upcoming* ...)

- K.G.H. Vollbrecht
- M.M. Wolf
- R.F. Werner

Distillation



Given

$\rho^{\otimes n}$

LOCC

Wanted

$$|\Omega\rangle\langle\Omega|^{\otimes m}$$

$$\Omega = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$$

Distillable Entanglement

$$E_D(\rho) = \frac{m}{n}$$

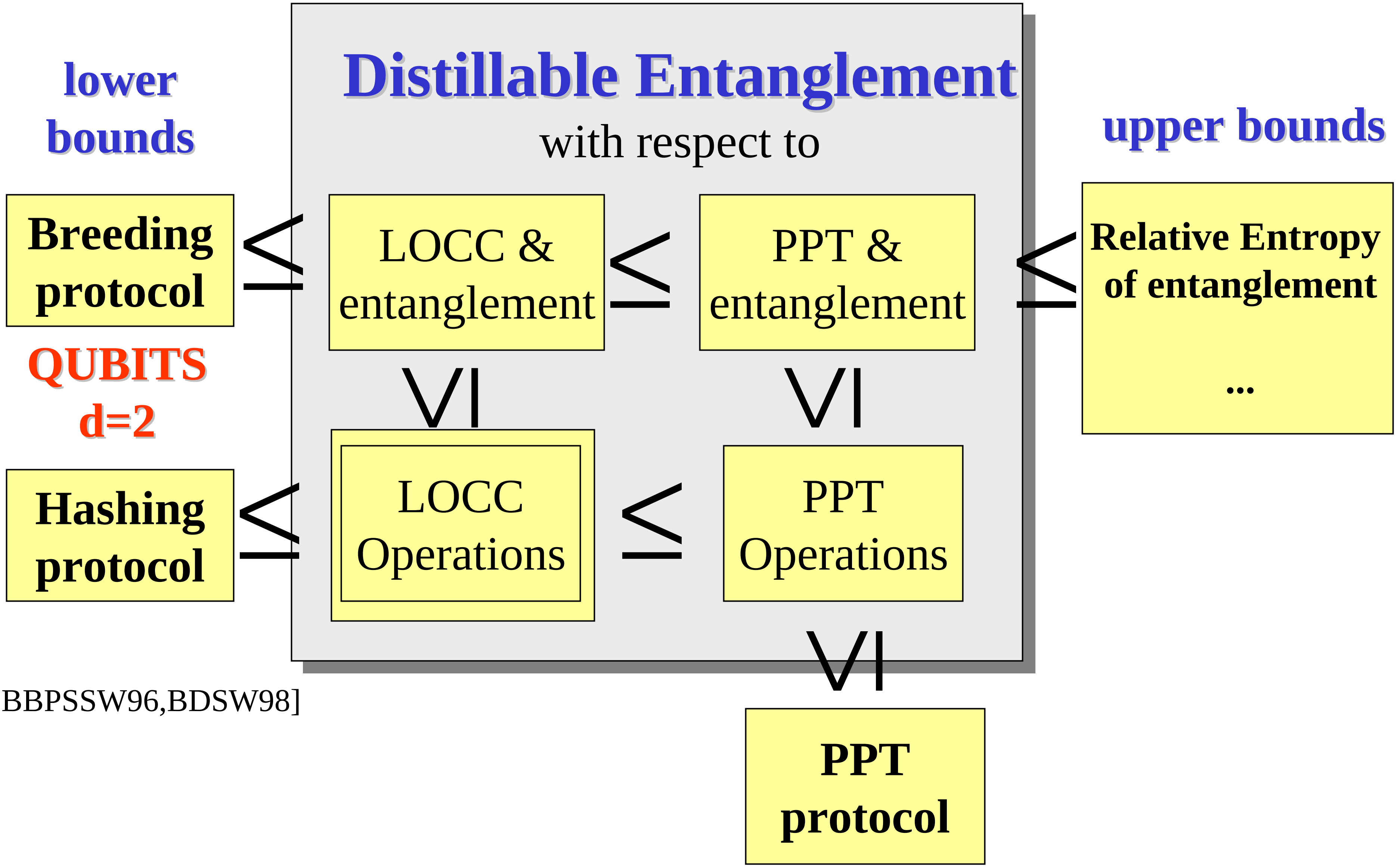
Optimization over all LOCC protocols

Asymptotic limit n→ infinity

Input: Alice and Bob share many copies of a mixed entangled state.

Operations: Alice and Bob are allowed to use **L**ocal **O**perations & **C**lassical **C**ommunication (**LOCC**)

Output: The goal is to create maximally entangled states (in the asymptotic limit)



lower bounds

Distillable Entanglement

with respect to

upper bounds

Breeding protocol ≤ LOCC & entanglement ≤ PPT & entanglement ≤ Relative Entropy of entanglement ...

QUBITS d=2

Hashing protocol ≤ LOCC Operations ≤ PPT Operations

PPT protocol

[BBPSSW96,BDSW98]

[Rains]

Outline

- Distillation
- Breeding
- Hashing
- low rank states

d-dimensional hashing/breeding

We need generalizations for:

Bell-States:

$$\psi_{00} = \frac{1}{\sqrt{2}}\left(|00\rangle + |11\rangle\right) \quad \psi_{01} = \frac{1}{\sqrt{2}}\left(|00\rangle - |11\rangle\right)$$

$$\psi_{10} = \frac{1}{\sqrt{2}}\left(|01\rangle + |10\rangle\right) \quad \psi_{11} = \frac{1}{\sqrt{2}}\left(|01\rangle - |10\rangle\right)$$

Bell-diagonal states:

$$\rho = \sum_{ij} \lambda_{ij} |\psi_{ij}\rangle\langle\psi_{ij}|$$

LOCC-Twirl:

$$T(\rho) = \frac{1}{4}\sum_i (\sigma_i \otimes \sigma_i)\rho(\sigma_i \otimes \sigma_i)^*$$

C-NOT

$$C|00\rangle = |00\rangle \quad C|10\rangle = |11\rangle$$

$$C|01\rangle = |01\rangle \quad C|11\rangle = |10\rangle$$

Generalization of Bell states

Bell states

➡

maximally entangled basis

„Bell-states“

Phase index

Addition modulo *d*

$$\psi_{kl} = \frac{1}{\sqrt{d}} \sum_{m} e^{\frac{2\pi i}{d} ml} \left| m, m+k \right\rangle$$

Shift index

„Bell-diagonal“-states:

$$\rho = \sum_{ij} \lambda_{ij} P_{ij}$$

$$P_{ij} = \left| \psi_{ij} \right\rangle \left\langle \psi_{ij} \right|$$

Generalization of C-NOT Gate

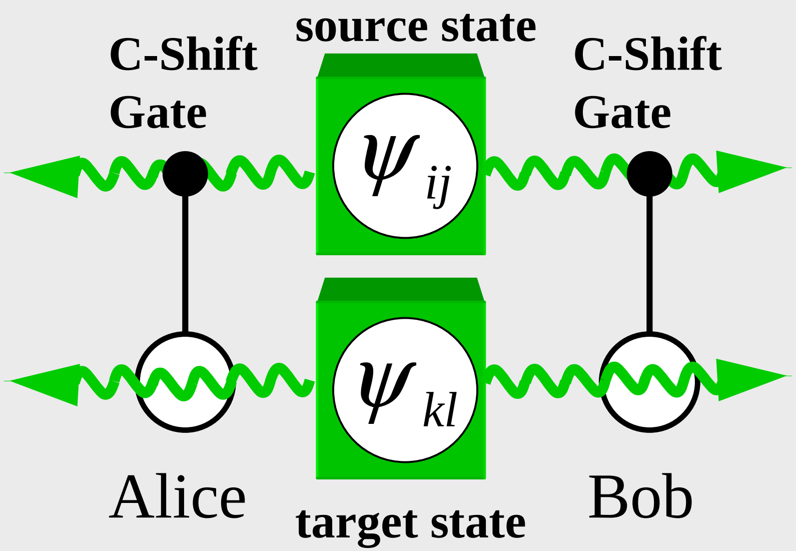
Controlled Shift

Controlled Not → Controlled Shift

C-Shift [Horodecki$^{\otimes 2}$99]

$$C|kl\rangle = |k, l+k\rangle$$

Bilateral C-Shift-operation (BCS) acting on Bell-states



Bilateral C-Shift

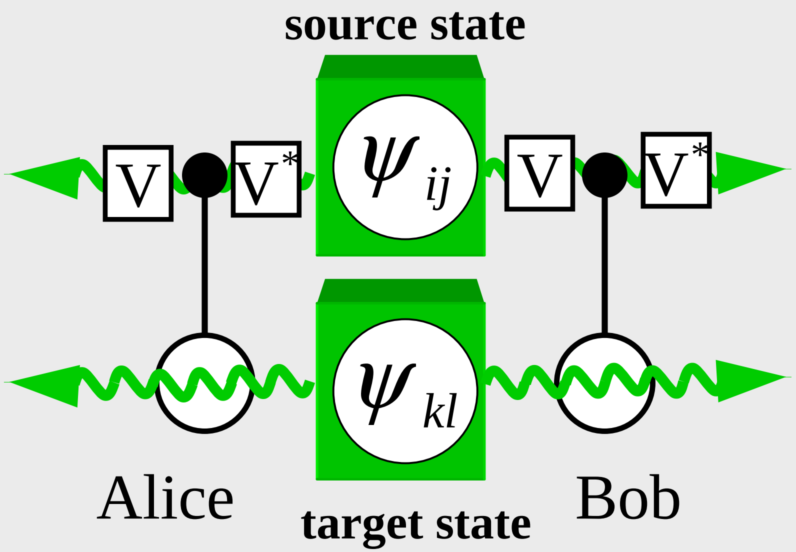
$$P_{ij} \otimes P_{kl} \to P_{i(j-l)} \otimes P_{(k+i)l}$$

Fourier transform

$$V|k\rangle = \sum_l e^{\frac{2\pi i}{d}kl}|l\rangle$$

$$\left(V \otimes V^*\right) P_{ij} \left(V \otimes V^*\right)^* = P_{j(-i)}$$

Bilateral Modified C-Shift-operation (MBCS) acting on Bell-states



Bilateral Modified C-Shift

$$P_{ij} \otimes P_{kl} \rightarrow P_{(i+l)j} \otimes P_{(k+j)l}$$

Generalized Twirl

$$U_{kl}|m\rangle = e^{\frac{2\pi i}{d}lm}|m+k\rangle$$

LOCC-Twirl

$$T(\rho) = \frac{1}{d^2}\sum_{kl}\left(U_{kl}\otimes U_{k(-l)}\right)\rho\left(U_{kl}\otimes U_{k(-l)}\right)^*$$

First step of the protocol:

Alice and Bob maps an arbitrary state ρ to a „Bell-diagonal state“

The main idea

Alice and Bob share *n* copies of the state *ρ.*

$$\rho^{\otimes n} = \underbrace{\sum_{i_1 j_1 \text{😐} i_n j_n}}_{\text{unknown}} \lambda_{i_1 j_1} \text{☹} \lambda_{i_n j_n} \underbrace{P_{i_1 j_1} \otimes \text{☹} \otimes P_{i_n j_n}}_{\text{Maximally entangled}}$$

Alice and Bob‘s strategy :

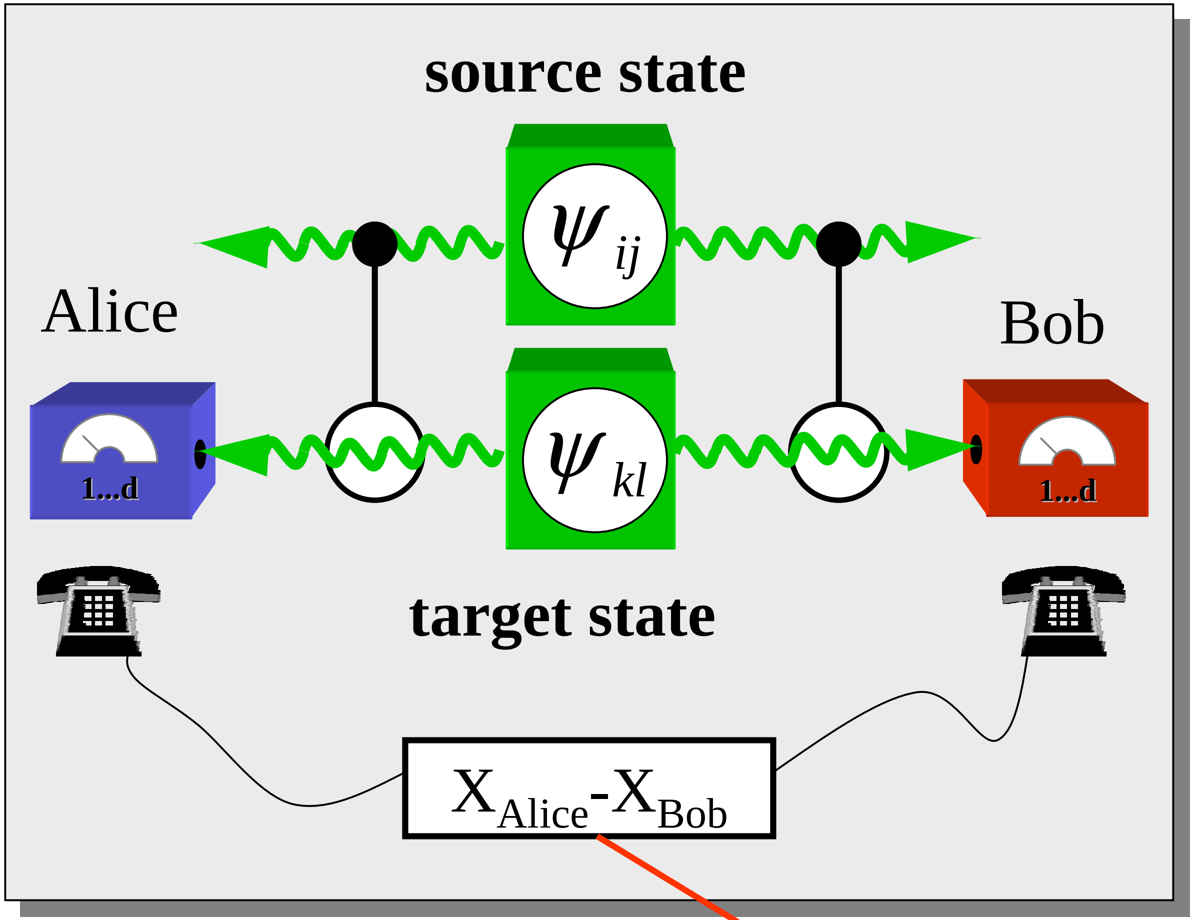
1. identify the index tuple

$$\overset{\sqcup}{S} = \{ i_1, j_1, i_2, j_2, \text{😐} i_n, j_n \}$$

2. Utilize

$$P^{\square}_{S} := P_{i_1 j_1} \otimes \text{☹} \otimes P_{i_n j_n}$$

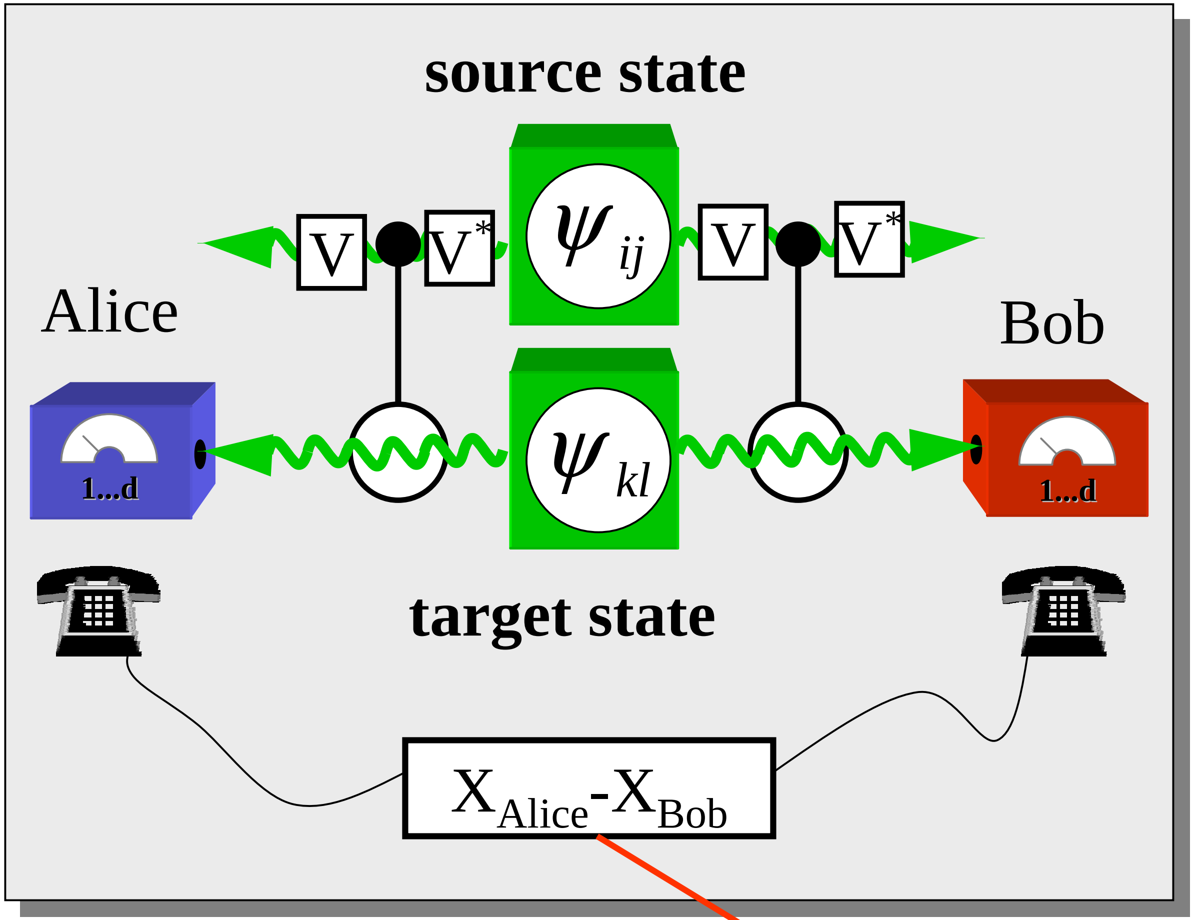
Breeding protocol with LOCC&entanglement



$$P_{ij} \otimes P_{k0} \rightarrow P_{ij} \otimes P_{(k+i)0}$$

If phase index of target state is zero

→ Source state stays unchanged

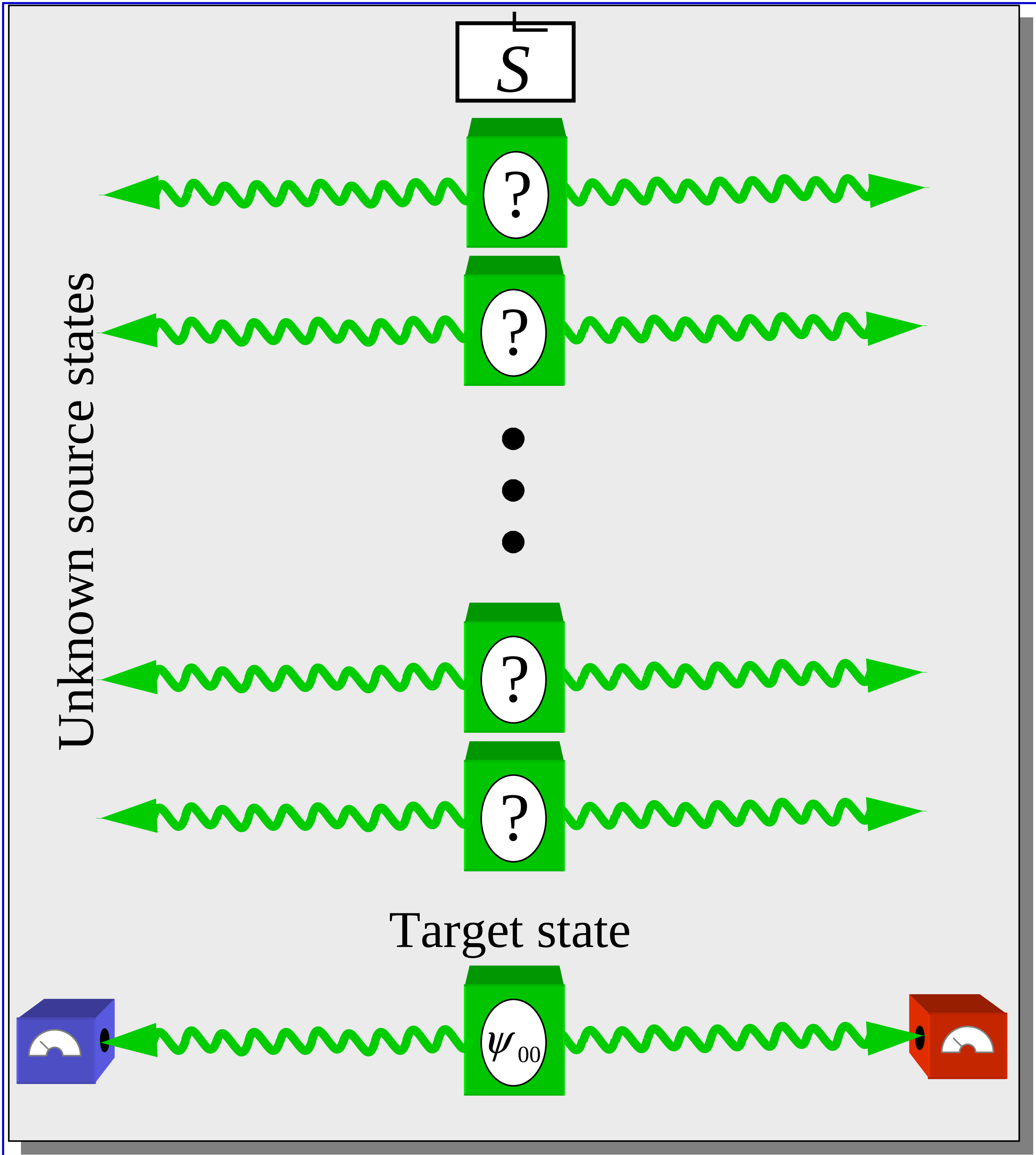


$$P_{ij} \otimes P_{k0} \rightarrow P_{ij} \otimes P_{(k+j)0}$$

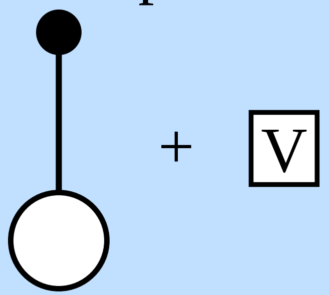
If phase index of target state is zero

➡ Source state stays unchanged

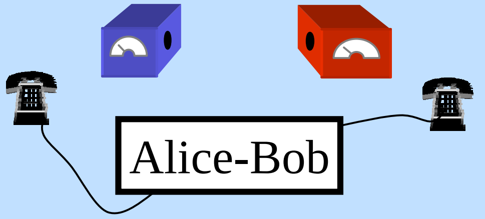
breeding



local operations



Classical communication

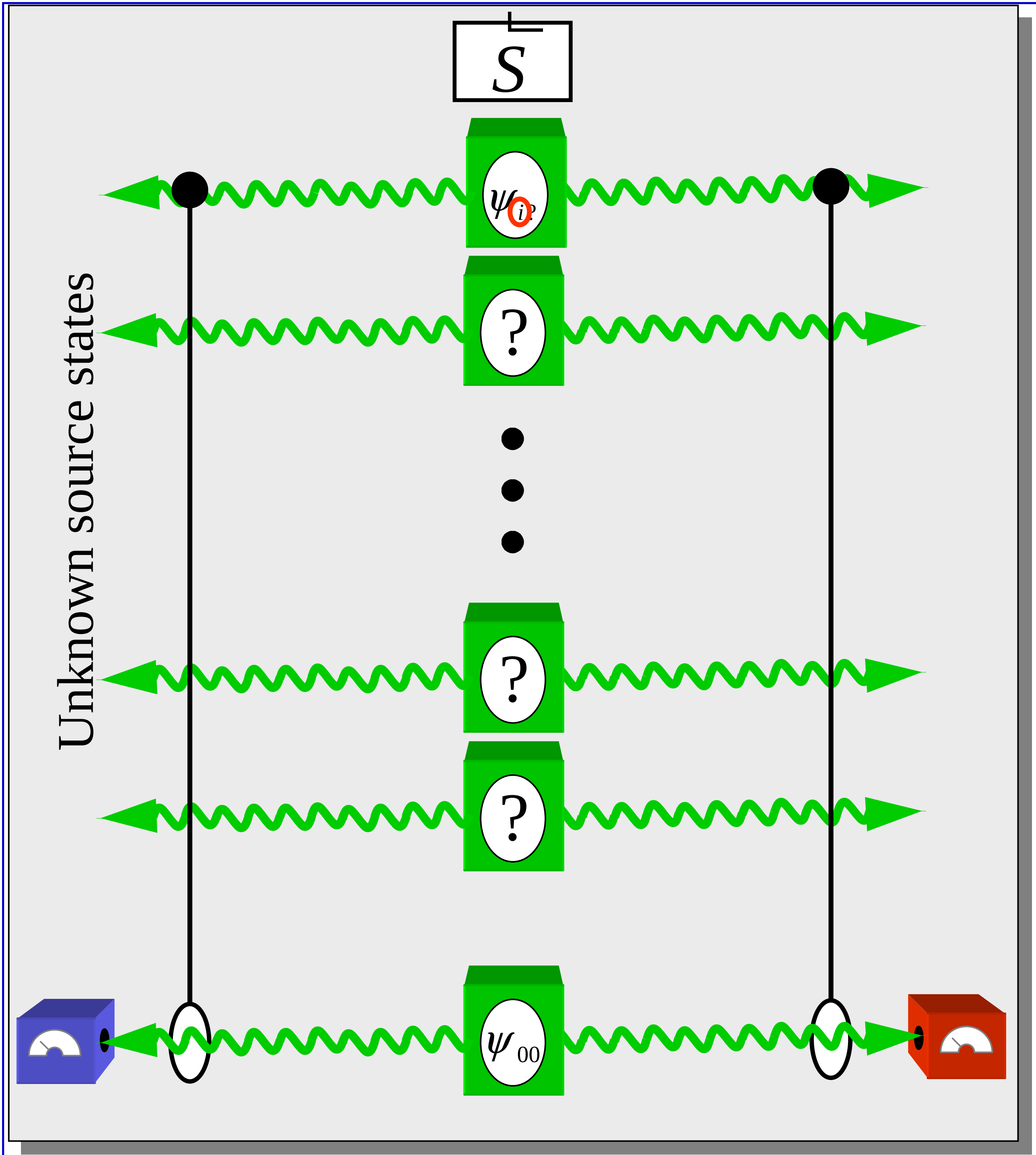


&

Extra entanglement

ψ_{00}

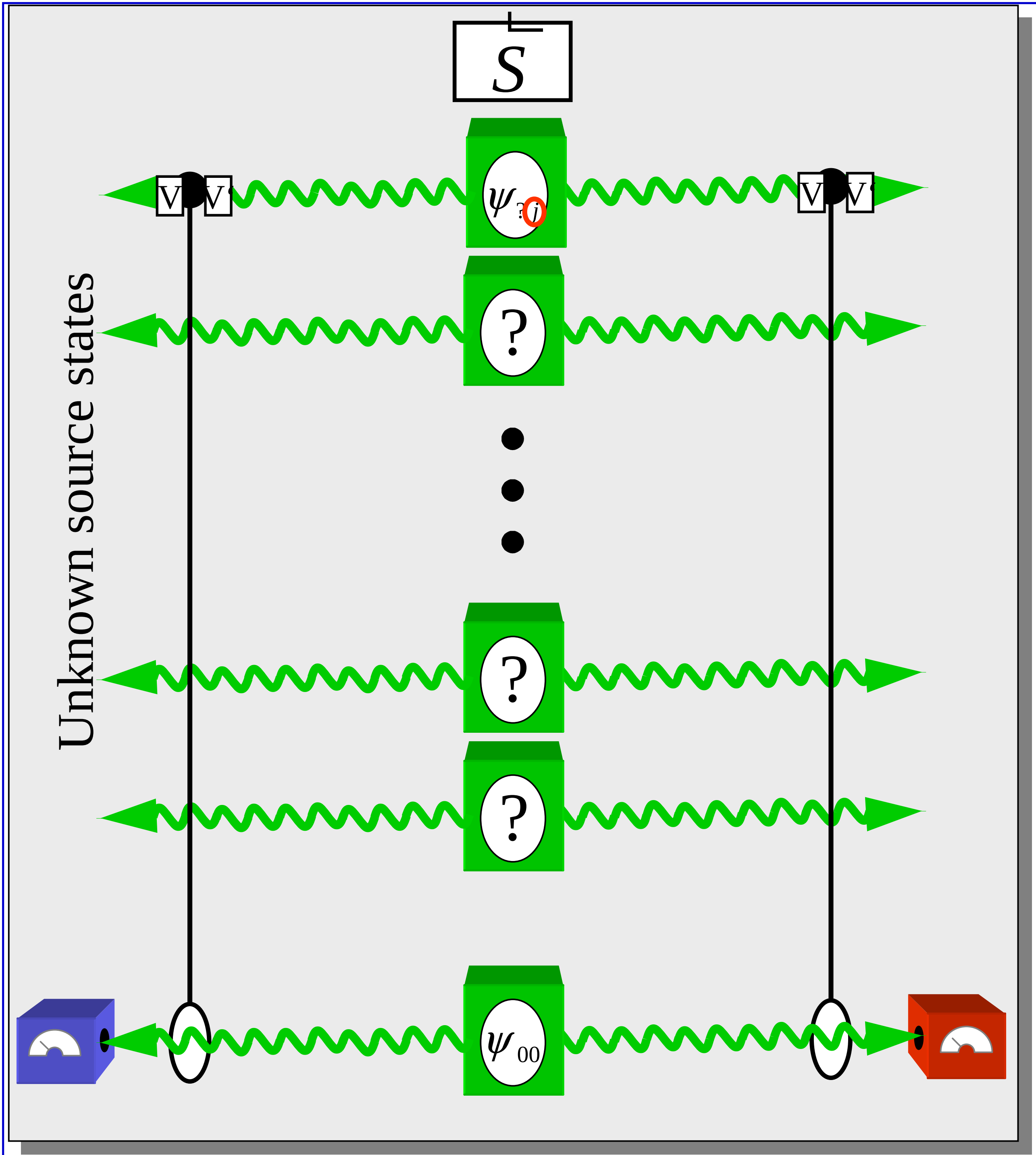
breeding



Result of measuring the target state

S_1

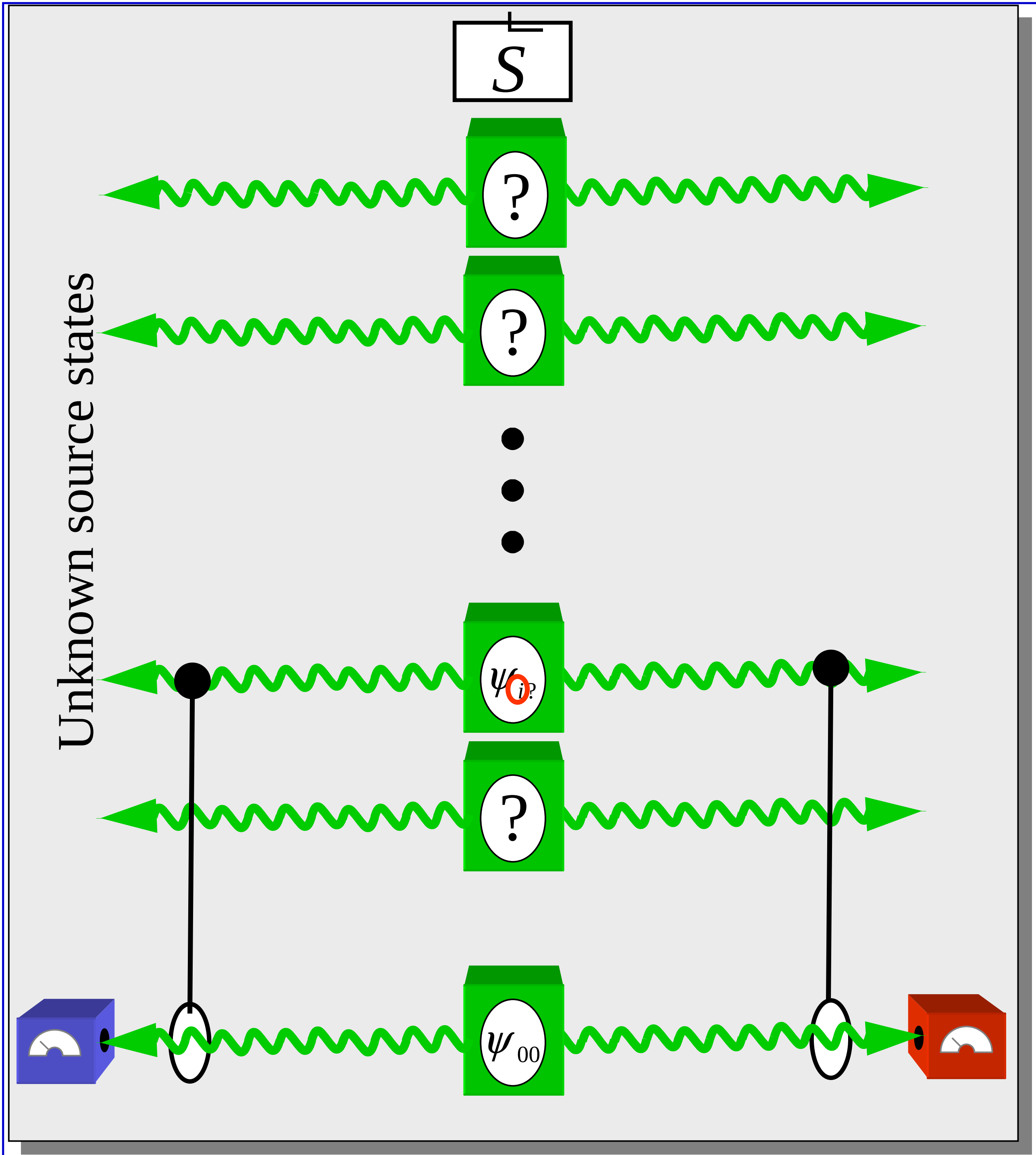
breeding



Result of measuring the target state

S_2

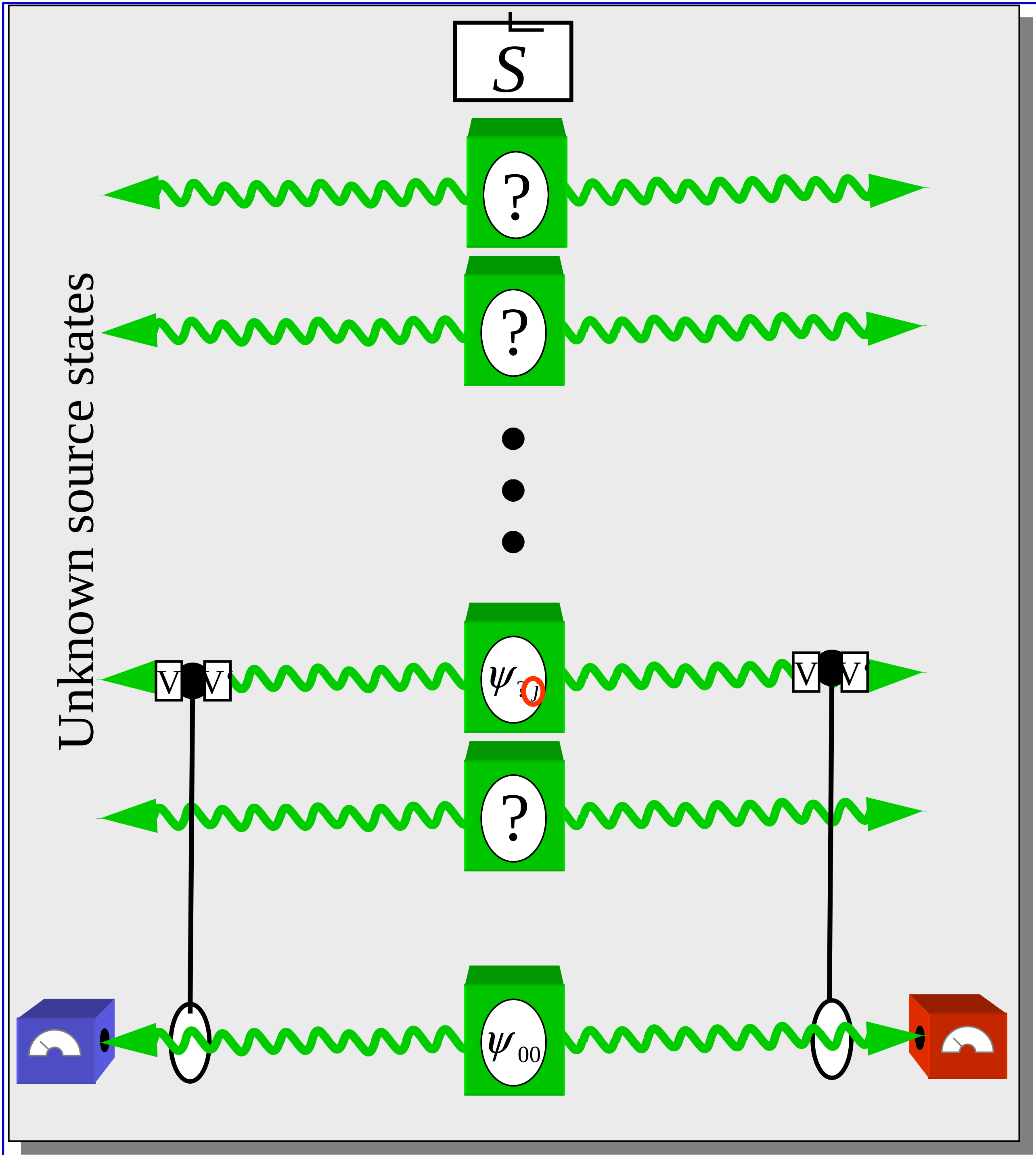
breeding



Result of measuring the target state

$$S_{2m-1}$$

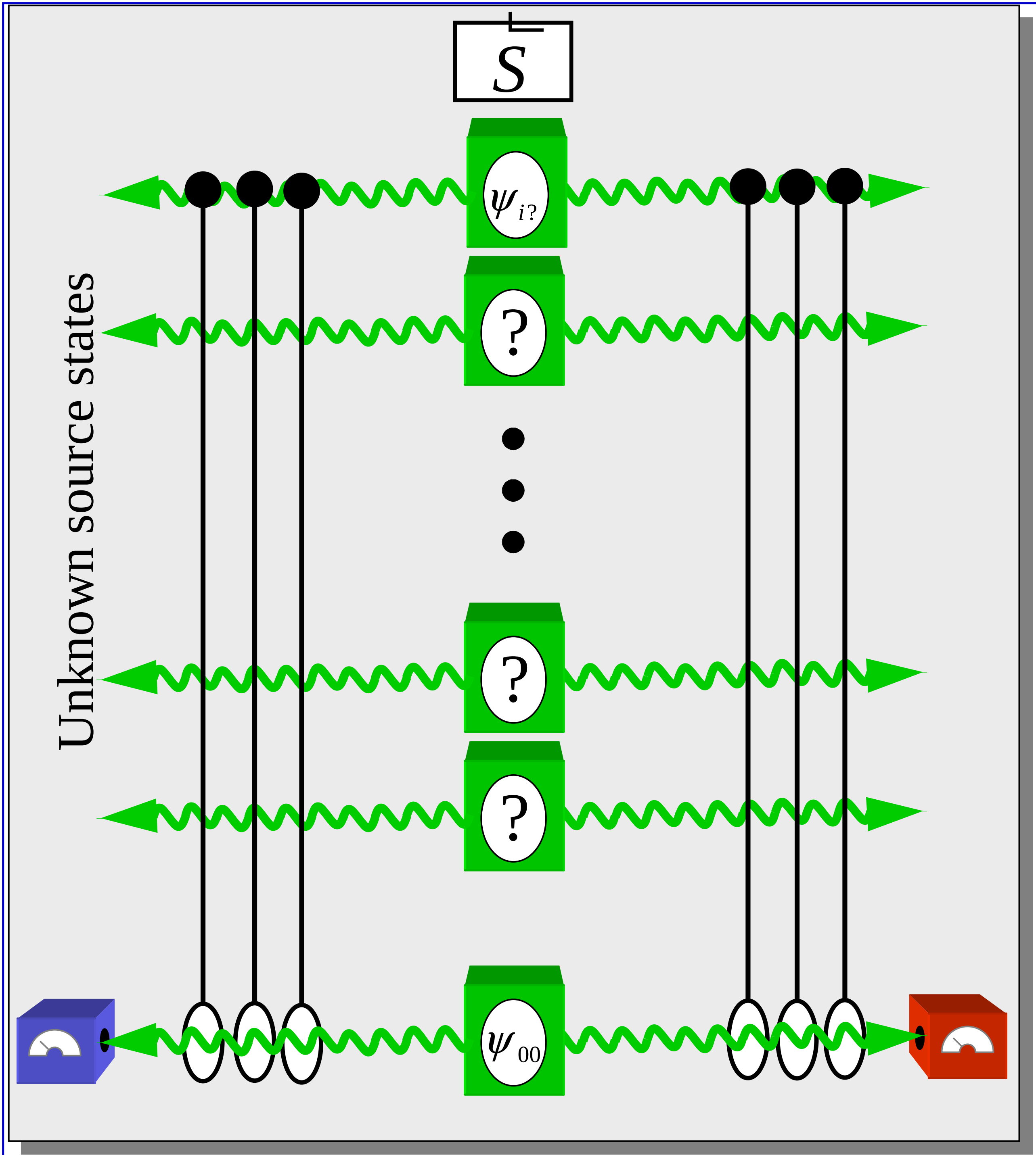
breeding



Result of measuring the target state

$$S_{2m}$$

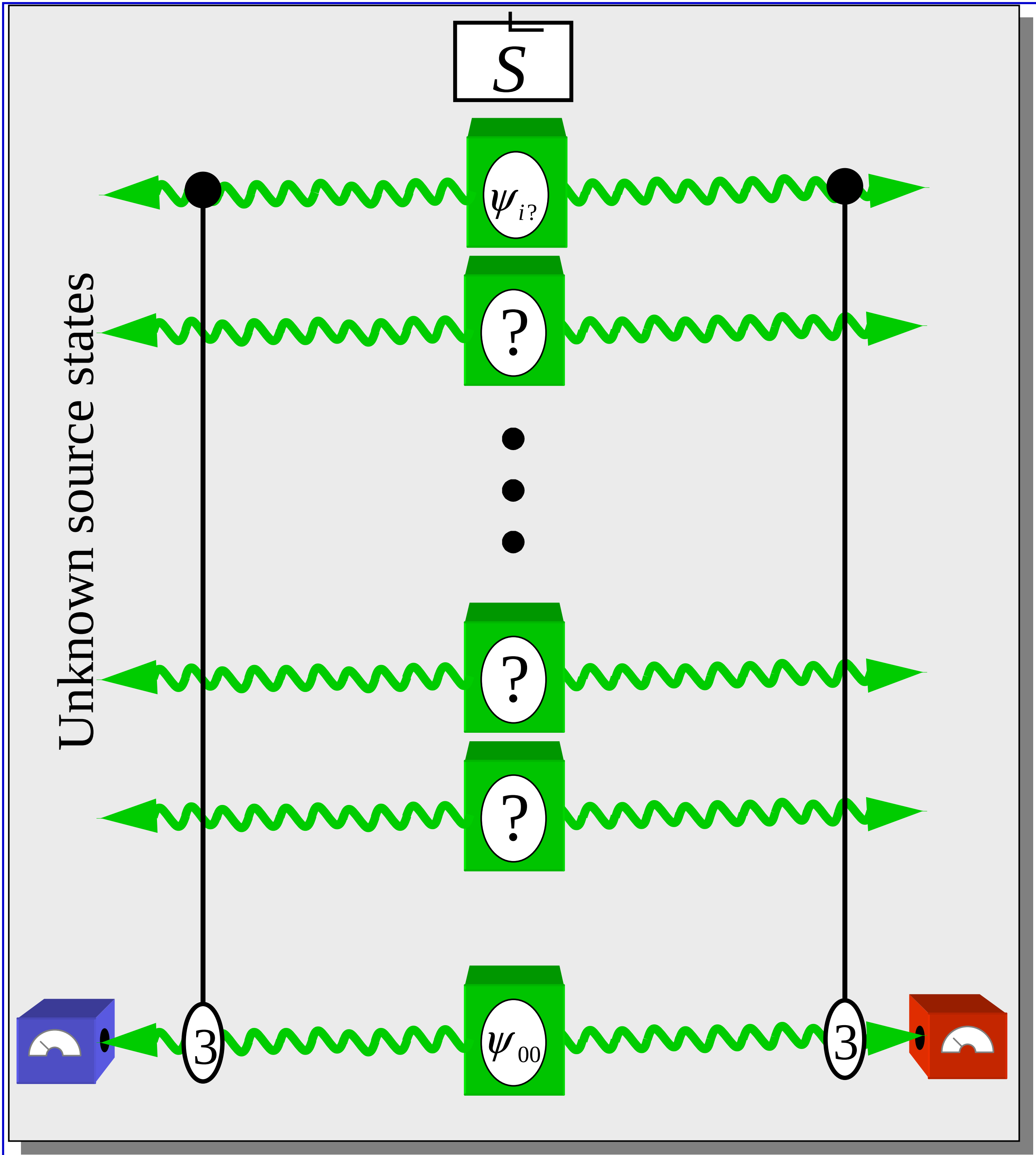
breeding



Result of measuring the target state

$$3 \cdot S_1$$

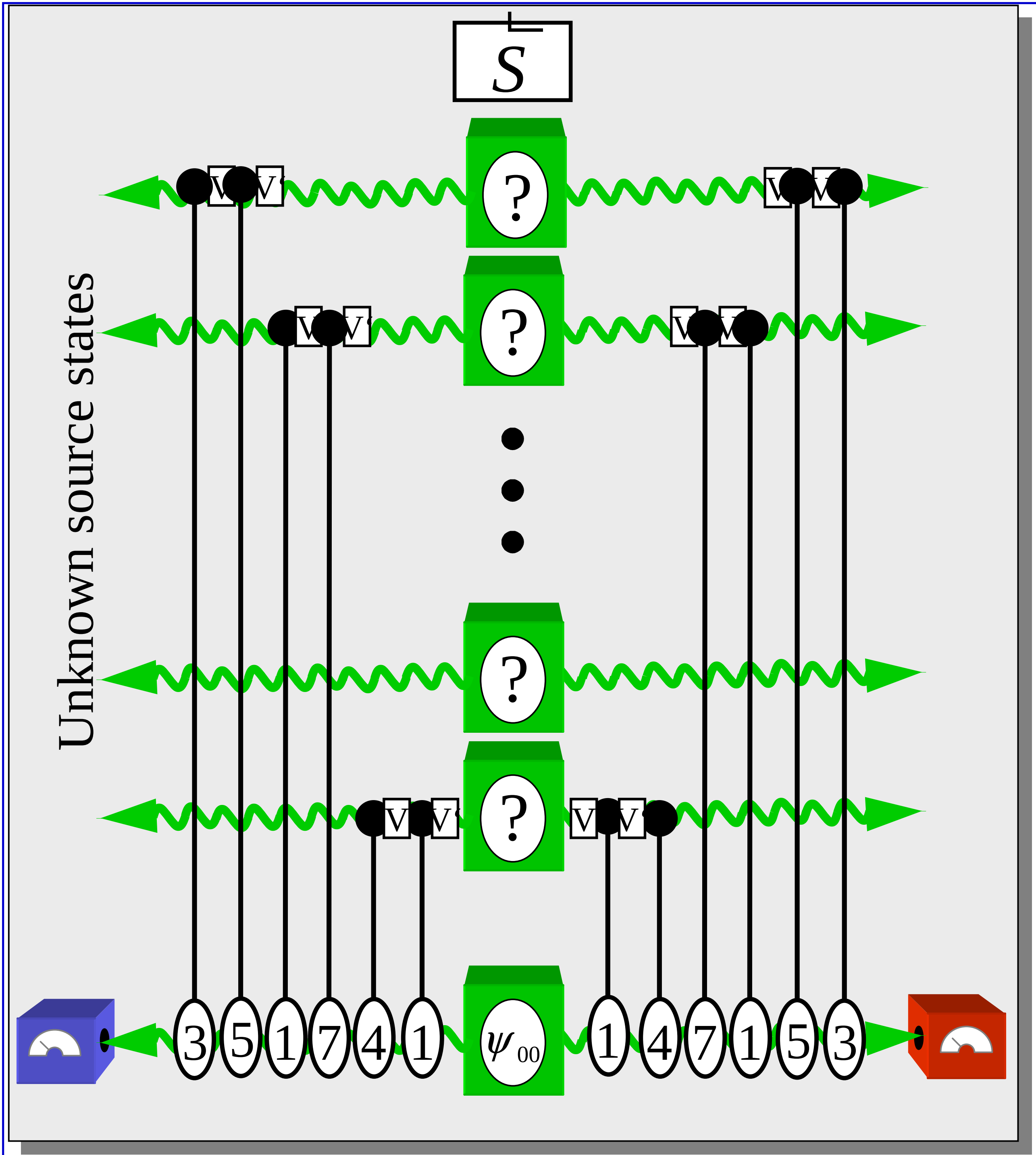
breeding



Result of measuring the target state

$$3 \cdot S_1$$

breeding



Sequence of BCS and MBCS is characterized by a vector

$$\vec{M} = \{3,5,17,☺ 4,1\}$$

Result of measuring the target state

$$\langle \vec{S} | \vec{M} \rangle = \sum_i S_i M_i$$

quantum problem → classical problem

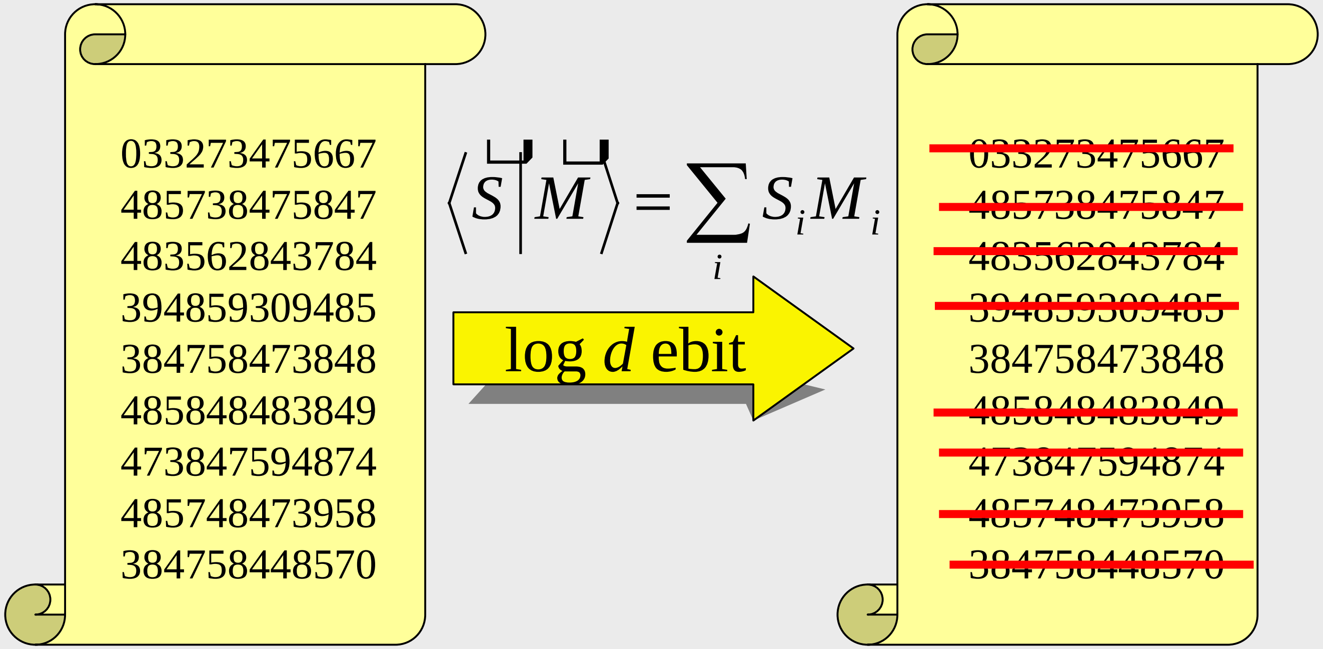
quantum state ρ → classical random variable $\{ij, \lambda_{ij}\}$

distill ρ → identify $\vec{S}$

LOCC & entanglement → $\langle \vec{S} | \vec{M} \rangle = \sum_i S_i M_i$

breeding

List of possible $\vec{S}$



033273475667
485738475847
483562843784
394859309485
384758473848
485848483849
473847594874
485748473958
384758448570

$$\langle \vec{S} | \vec{M} \rangle = \sum_i S_i M_i$$

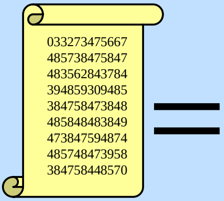
log *d* ebit

~~033273475667~~
~~485738475847~~
~~483562843784~~
~~394859309485~~
384758473848
~~485848483849~~
~~473847594874~~
~~485748473958~~
~~384758448570~~

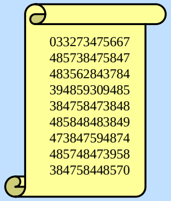
Repeat until S is known

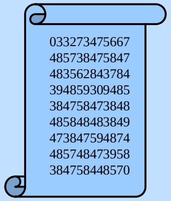
How many measurements are needed ?
How many S are on the list ?
How to choose M ?

How many S are on the list ?

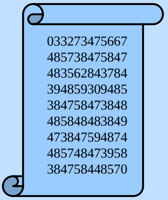
$\#$ 

$= 2^{n \log \mathrm{Rank}(\rho)}$

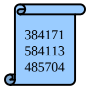


$=$


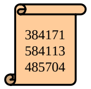
$+$

$\#$ 

$= 2^{n\,\mathrm{S}(\rho)}$

typical codewords $P(S \in$ 

$) \xrightarrow{n \to \infty} 1$

non-typical codewords $P(S \in$ 

$) \xrightarrow{n \to \infty} 0$

How to choose M ?

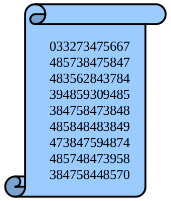
Choose M completely random !

This turns out to be optimal in the asymptotic limit.

In each step the number of codewords is reduced by a factor 1/d

breeding rate

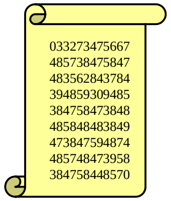
$$E_D(\rho) \geq \log_2 d - S(\rho)$$



Maximally entangled states only in the asymptotic limit

rate

$$\log_2 d - \log_2 \mathrm{Rank}(\rho)$$



Maximally entangled states for finite *n*

IF

d is prime (or power of a prime)

$$b = a \cdot x \quad \bmod d \qquad a \neq 0$$

The equation has a unique solution for *x* if and only if *d* is prime.

This guarantees that Alice and Bob gain log *d* bits of information in every step.

$$P\left(\langle \vec{M} | \vec{S}_1 \rangle = \langle \vec{M} | \vec{S}_2 \rangle\right) = \frac{1}{d}$$

$$\vec{M} = \text{random}$$

Way out:

Let the target state live in prime dimension

n copies

$$\rho \in B(C^{d} \otimes C^{d})$$

&

Extra entanglement

$$\psi_{oo} \in C^{d'} \otimes C^{d'}$$

C-Shift

$$C|kl\rangle = |k, l+k\rangle$$

$$\in C^{d} \otimes C^{d'}$$

d´ is prime

Bilateral C-Shift

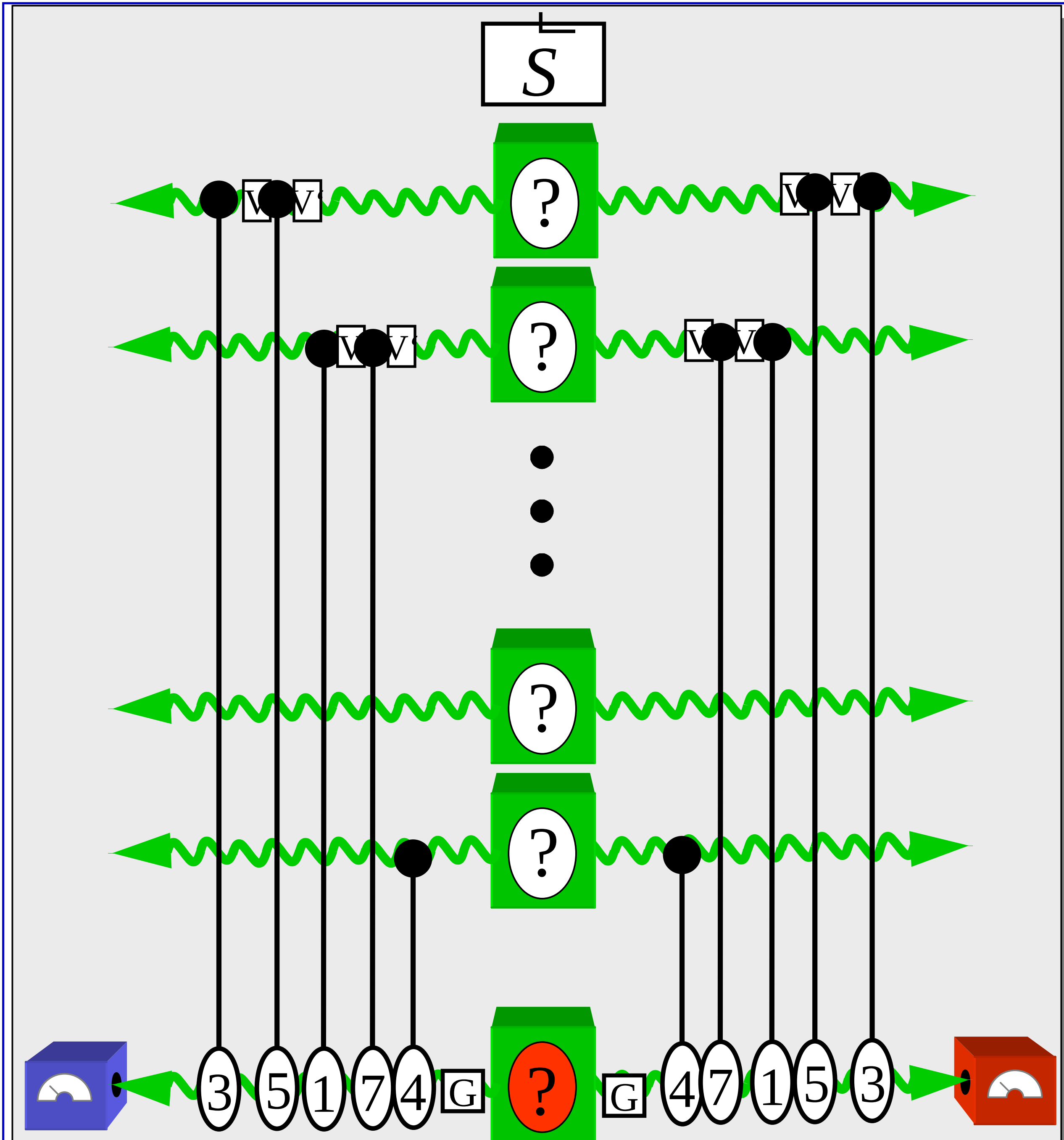
$$\xcancel{P_{ij} \otimes P_{kl} \to P_{(i+l)j} \otimes P_{(k+j)l}}$$

BUT

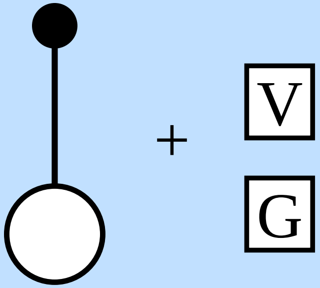
$$P_{ij} \otimes P_{k0} \to P_{ij} \otimes P_{(k+j)0}$$

Hashing protocol
with
LOCC

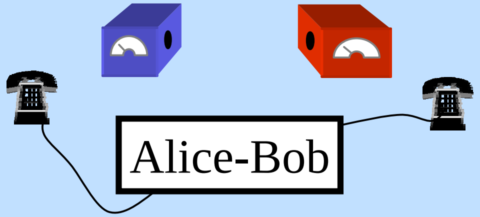
hashing



local operations



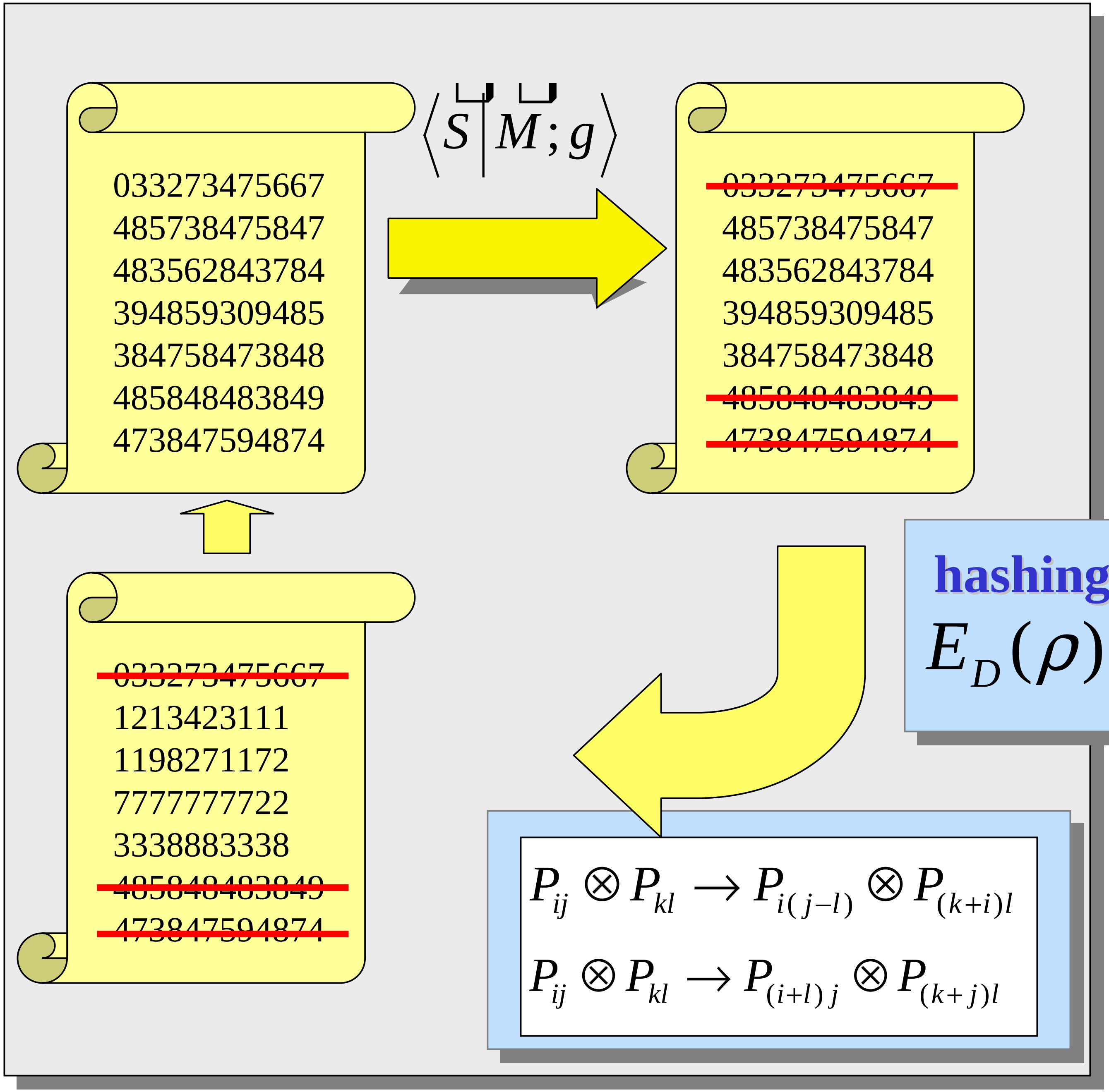
Classical communication



Result of measuring the target state

$$\langle \vec{S} | \vec{M}; g \rangle = \langle \vec{S} | \vec{M} \rangle + \sum_i M_{2i} M_{2i-1} S_{2n} + S_{2n-1} + g S_{2n}$$

hashing



$\langle \overline{S} | \overline{M} ; g \rangle$

033273475667
485738475847
483562843784
394859309485
384758473848
485848483849
473847594874

~~033273475667~~
485738475847
483562843784
394859309485
384758473848
~~485848483849~~
~~473847594874~~

~~033273475667~~
1213423111
1198271172
7777777722
3338883338
~~485848483849~~
~~473847594874~~

$$P_{ij} \otimes P_{kl} \rightarrow P_{i(j-l)} \otimes P_{(k+i)l}$$

$$P_{ij} \otimes P_{kl} \rightarrow P_{(i+l)j} \otimes P_{(k+j)l}$$

hashing rate

$$E_D(\rho) \geq \log_2 d - S(\rho)$$

iff d is prime (or power of a prime)

Summary: Distillation

For d prime (or power of prime): LOCC protocol

For arbitrary dimension LOCC&entanglement protocol

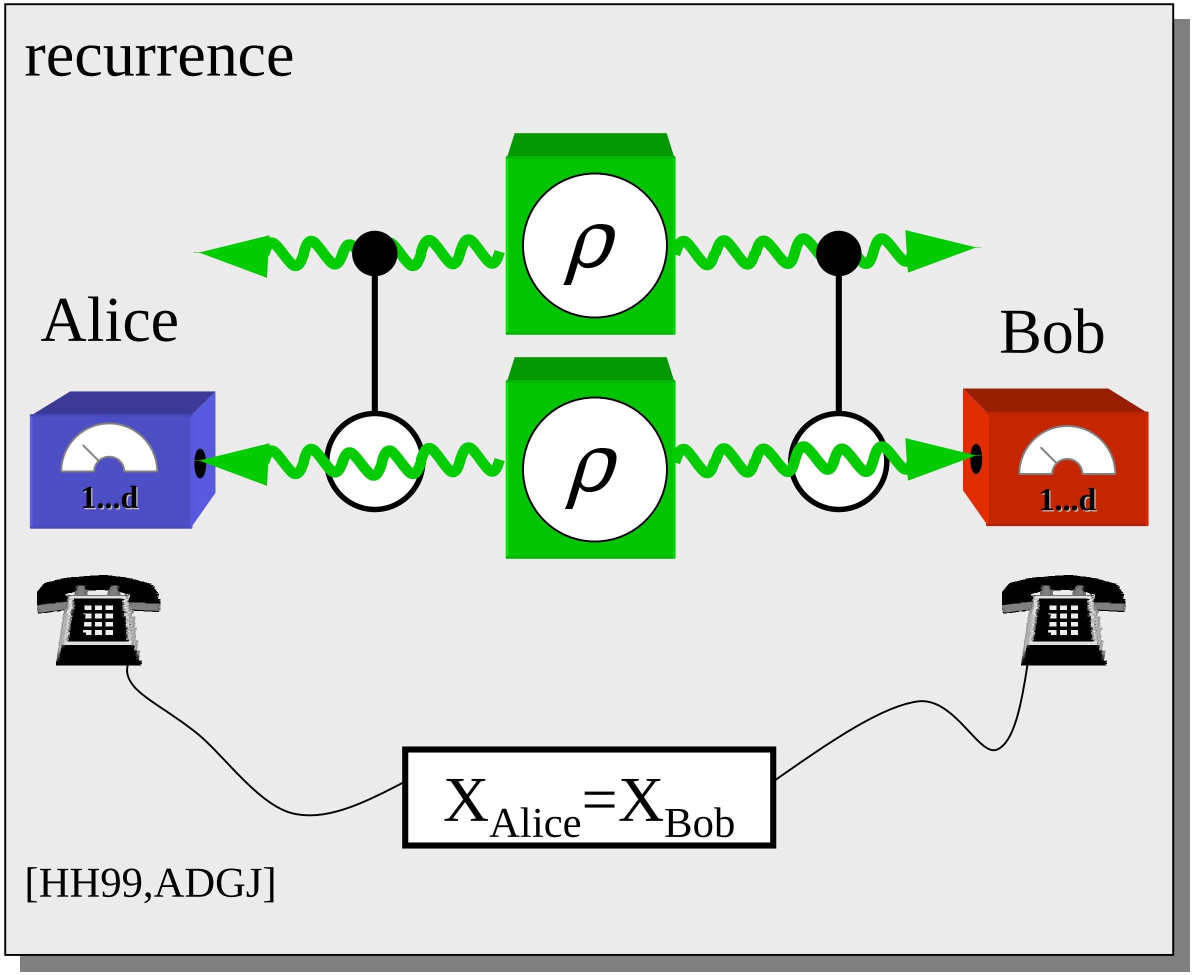
hashing/breeding rate

$$E_D(\rho) \geq \log_2 d - S(\rho)$$

For Rank(ρ)<d we get a positive rate for finite *n*.

$$\log_2 d - \log_2 \mathrm{Rank}(\rho) - \varepsilon$$

Further optimization



recurrence

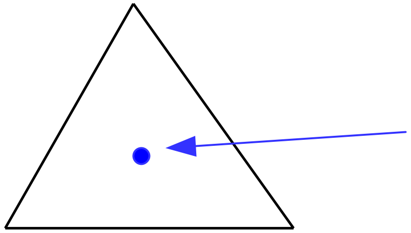
[HH99,ADGJ]

Optimality for low rank states

Consider the (d-1) parameter family:

$$\rho = \sum_l \lambda_l |\psi_l\rangle\langle\psi_l|$$

$$\psi_l := \psi_{0l}$$



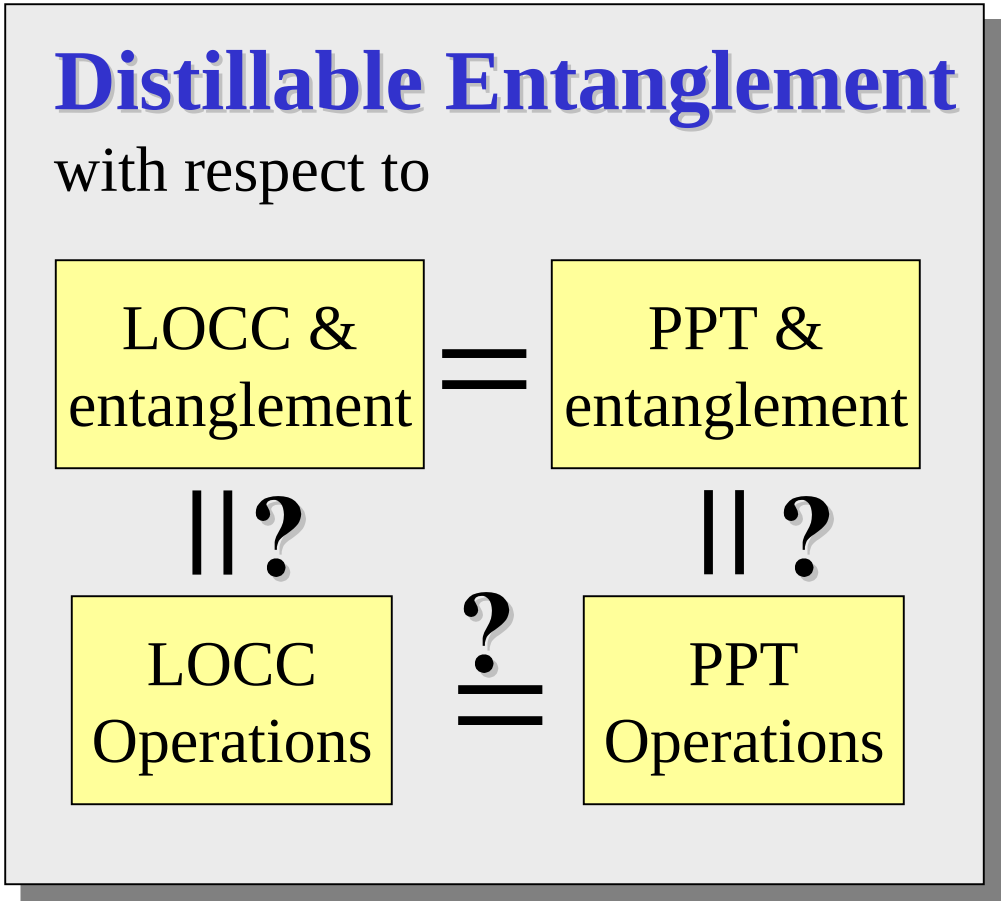
barycenter is the only separable state and is nearest in RelEnt distance :

$$E_{RE}(\rho) = \inf_{\sigma_{sep}} \mathrm{tr}\, \rho\left(\log\rho - \log\sigma_{sep}\right)$$

$$\log_2 d - S(\rho) = E_{RE} \geq E_D \geq \log_2 d - S(\rho)$$

The obtained rate is equal to the Distillable Entanglement !

$$\rho = \sum_{l} \lambda_l |\psi_l\rangle\langle\psi_l|$$



Distillable Entanglement

with respect to

LOCC & entanglement $=$ PPT & entanglement

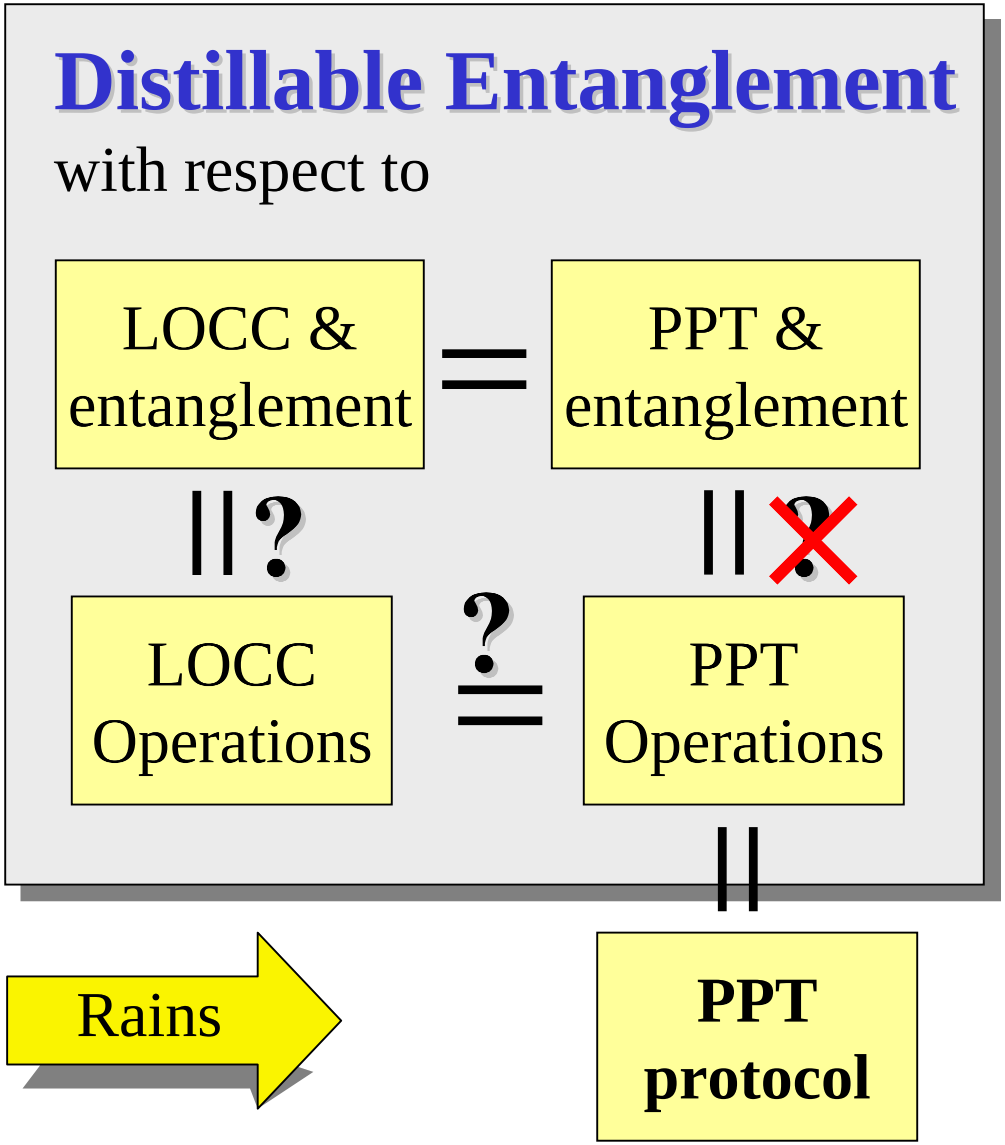
$\|$? $\|$?

LOCC Operations $\overset{?}{=}$ PPT Operations

$$\rho = \sum_l \lambda_l |\psi_l\rangle\langle\psi_l|$$

$$\rho = \sum_l a_{ij} |ii\rangle\langle jj|$$

Maximal correlated



Distillable Entanglement

with respect to

LOCC & entanglement = PPT & entanglement

$\|?$

$\|\cancel{?}$

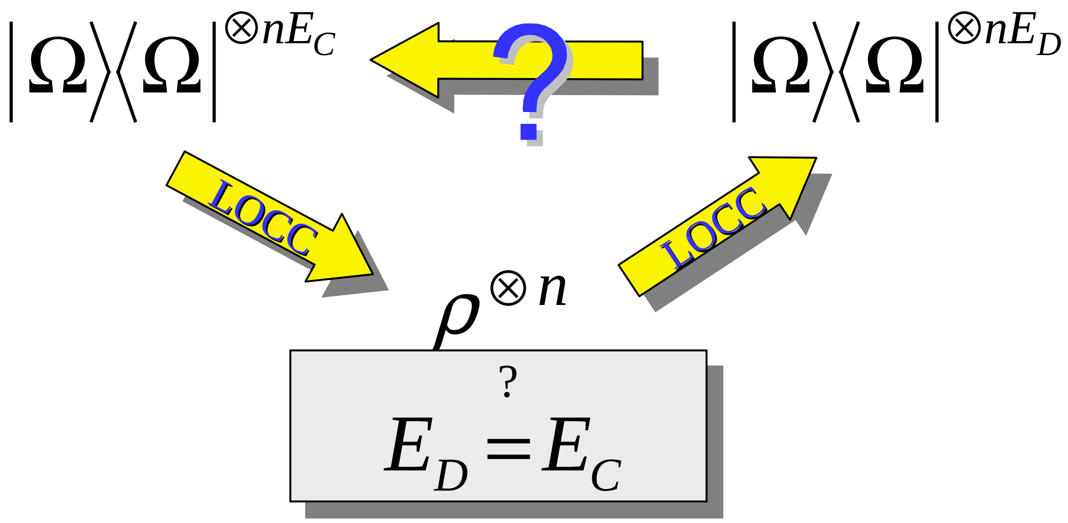
LOCC Operations $\overset{?}{=}$ PPT Operations

$\|$

Rains

PPT protocol

Irreversibility of Entanglement



$$|\Omega\rangle\langle\Omega|^{\otimes nE_C}$$

$$|\Omega\rangle\langle\Omega|^{\otimes nE_D}$$

?

$$\rho^{\otimes n}$$

$$E_D \overset{?}{=} E_C$$

Vidal & Cirac: counter-examples !

For the whole (d-1) parameter family:

- Irreversibility is generic !
- All reversible states are “pseudo-pure“

pseudo-pure

All pure state entanglement can be extracted by a simple operation on a single copy.

Example:

$$\rho = \sum_i \left|\psi_i{}^{AB}\right\rangle\left\langle\psi_i{}^{AB}\right| \otimes |i\rangle\langle i|^A \otimes |i\rangle\langle i|^B$$

$$\rho = \left|\psi^{AB}\right\rangle\left\langle\psi^{AB}\right| \otimes \rho_{sep}^{AB}$$

Entanglement cost

$$\rho = \sum_l \lambda_l |\psi_l\rangle\langle\psi_l|$$

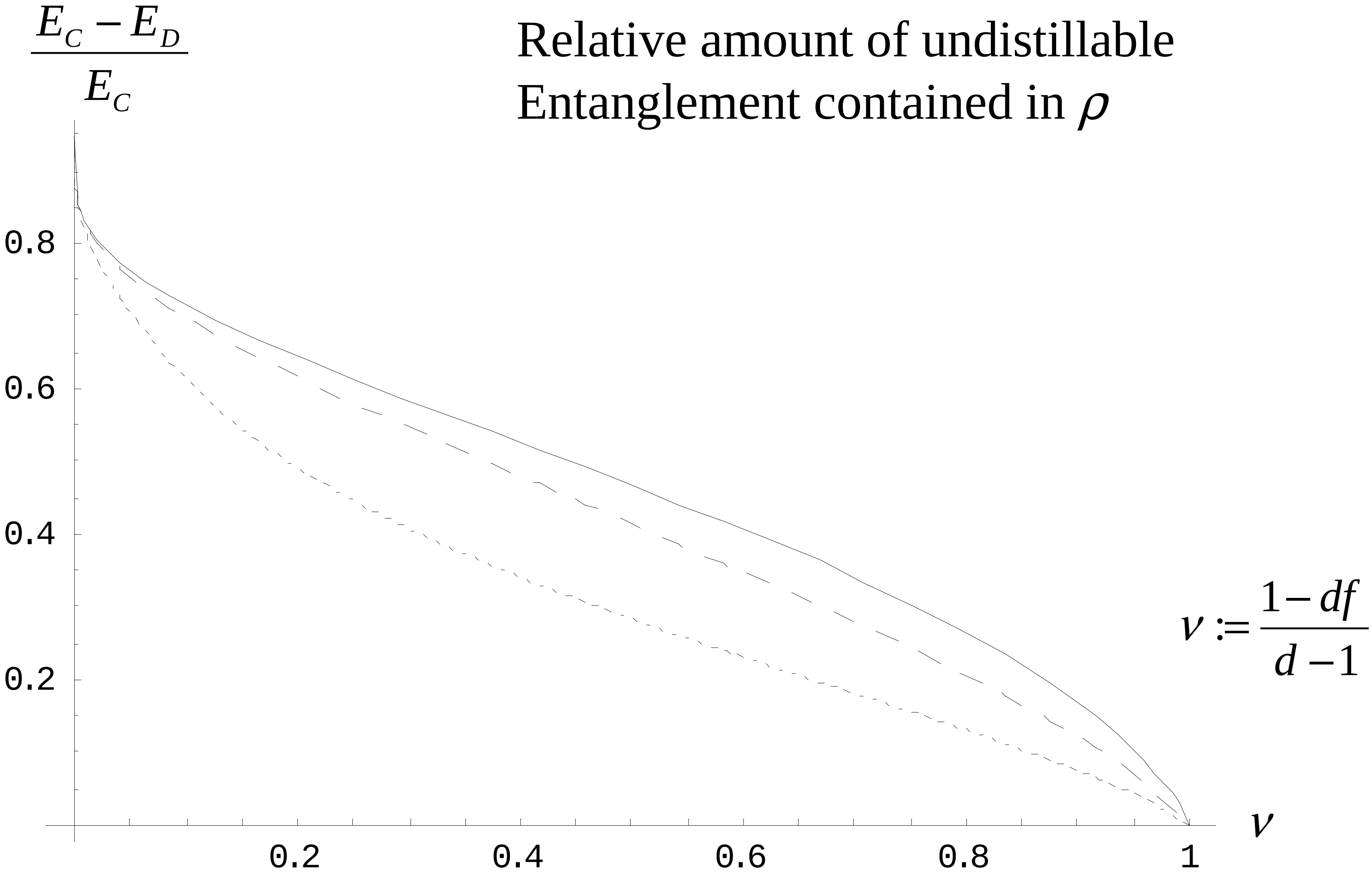
→ Entanglement cost is equal to
Entanglement of formation

$$\rho = f|\psi_0\rangle\langle\psi_0| + \frac{1-f}{d-1}\sum_{l=1}^{d-1} |\psi_l\rangle\langle\psi_l|$$

→ Entanglement of formation is equal to the
Entanglement of formation of a isotropic state

$$\rho = f|\psi_0\rangle\langle\psi_0| + \frac{1-f}{d^2-1}(\mathbf{1} - |\psi_0\rangle\langle\psi_0|)$$

Relative amount of undistillable Entanglement contained in ρ



$$\nu := \frac{1 - df}{d - 1}$$

$$d = 2,10,100$$

Conclusion

- Generalization of hashing/breeding protocol
- new class of low rank states
- irreversibility is generic