Hiding Quantum Data

Cast:

Charles Bennett………….. Hagrid
David DiVincenzo…………Han Solo
Patrick Hayden……………. Narrator
Debbie Leung…………….. Hermione
Peter Shor…………………. Dumbledore
Barbara Terhal…………….Princess Leia
Andreas Winter……………Harry Potter

An IBM-IQI-MSRI-AT&T Production

Overview

- Act I

- LOCC data hiding for quantum states

(quant-ph/0207147)

- Act II

- From RSP to PQC to data hiding

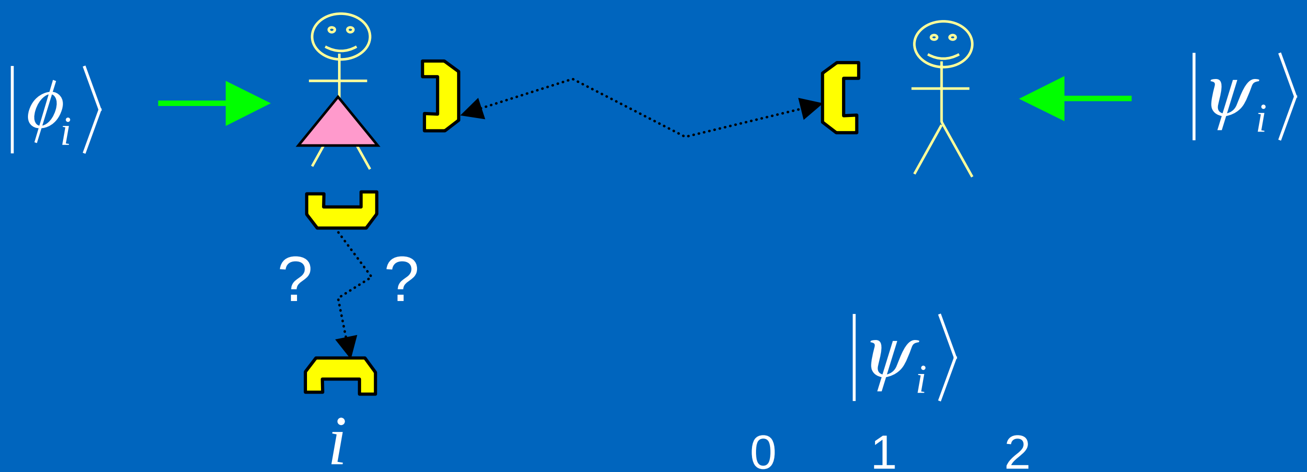
A few years ago in

a lab moderately

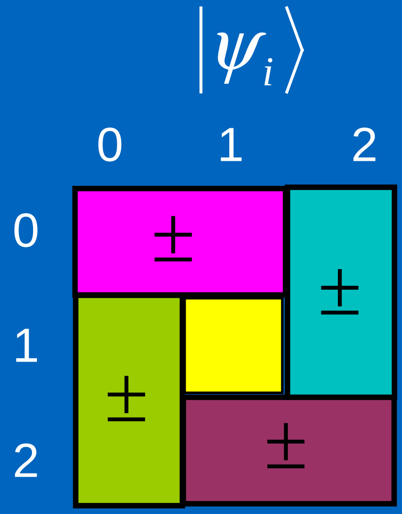
far away...

Nonlocality without entanglement

$$\langle \phi_i \psi_i | \phi_j \psi_j \rangle = \delta_{ij}$$



Not always possible: $|\phi_i\rangle$

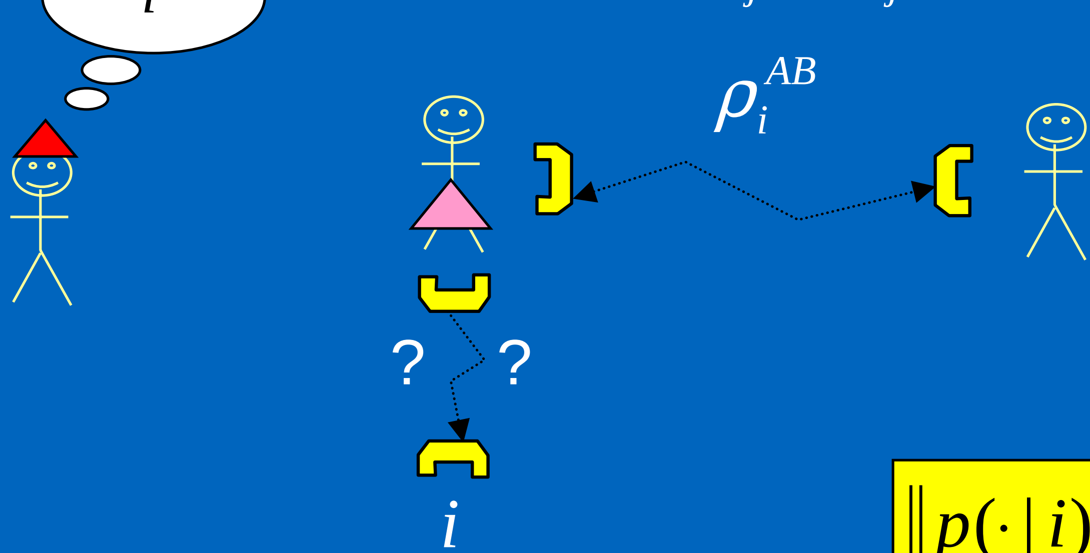


[BDFMRSSW, 1999]

Quantum data hiding

GOAL: Charlie hides a bit from Alice and Bob, secure against LOCC

$$\mathrm{tr}\,\rho_i \rho_j = \delta_{ij}$$



$$\left\| p(\cdot \mid i) - p(\cdot \mid j) \right\|_1 < \varepsilon$$

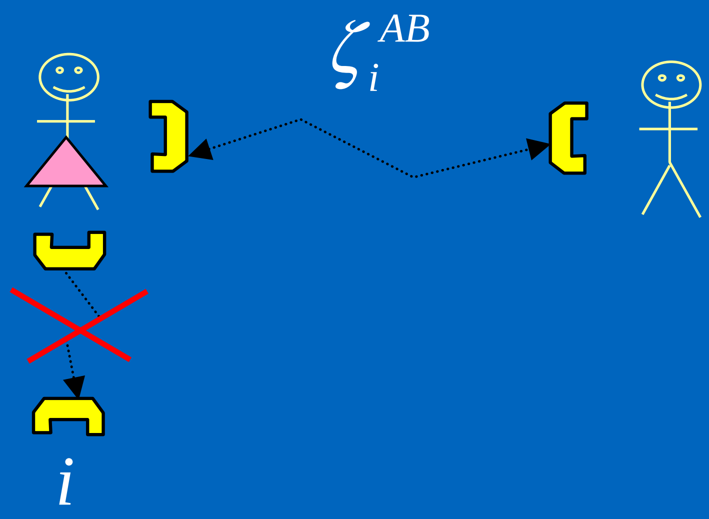
RESULT: There exist bipartite n-qubit states hiding a bit with security $2^{-(n-1)}$.

[DLT, 2001]

Hiding a qubit: First attempt

TASK: Hide an arbitrary quantum state $|\varphi\rangle = \alpha|0\rangle + \beta|1\rangle$

$$\langle \zeta_i | \zeta_j \rangle = \delta_{ij}$$



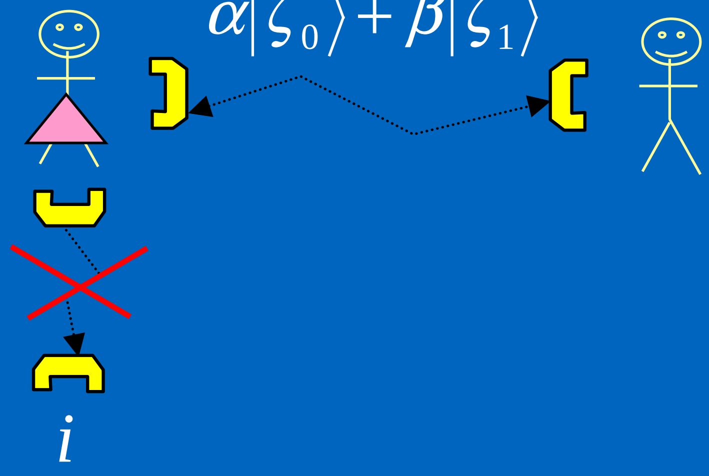
Prepare superpositions of well hidden states?

Hiding a qubit: First attempt

TASK: Hide an arbitrary quantum state $|\varphi\rangle = \alpha|0\rangle + \beta|1\rangle$

$$\langle \zeta_i | \zeta_j \rangle = \delta_{ij}$$

$$\alpha|\zeta_0\rangle + \beta|\zeta_1\rangle$$



PROBLEM: Data hiding with pure states is impossible!
(So much for superpositions.)

[WSHV,2000]

2nd simplest idea

THE PLAN: Use classical hidden bits as key to randomize a qubit

$$E(\varphi) = \frac{1}{4}\sum_{i=0}^{3} \rho_i^{AB_1} \otimes \sigma_i \varphi \sigma_i^{B_2}$$

PROPERTIES: 1) φ can be recovered using quantum communication
2) Naïve attacks fail (AB_1 to find key then rotate B_2)

PROBLEM: Alice and Bob can attack AB_1B_2

Actually, *not* a problem

Any method to learn about φ by LOCC will provide a method to defeat the original cbit hiding scheme.

Will argue the contrapositive:

Assume there is an LOCC operation L (with output on Bob's system alone) and two input states to the hiding map E such that

$$L\left(E\left(\varphi_0\right)\right) \neq L\left(E\left(\varphi_1\right)\right)$$

Minor algebra

$$L(E(\varphi)) = L\left(\tfrac{1}{4} \sum_{i=0}^{3} \rho_i^{AB_1} \otimes \sigma_i \varphi \sigma_i^{B_2} \right)$$

$$= \tfrac{1}{4} \sum_{i=0}^{3} L_i(\sigma_i \varphi \sigma_i), \quad \text{where } L_i(\omega) = L\left(\rho_i^{AB_1} \otimes \omega^{B_2}\right)$$

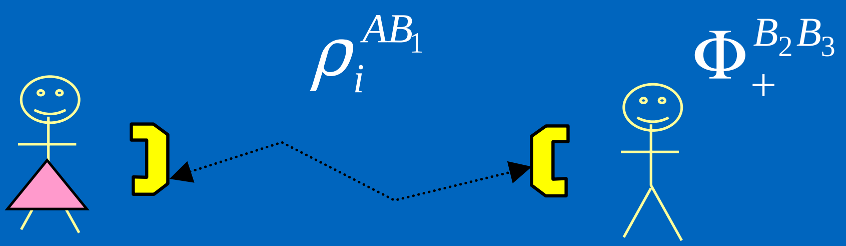
CLAIM: Not all L_i can be the same TPCP map. If they were, then by linearity:

$$L(E(\varphi)) = \tfrac{1}{4} \sum_{i=0}^{3} L_0(\sigma_i \varphi \sigma_i) = L_0\left(\tfrac{1}{4} \sum_{i=0}^{3} \sigma_i \varphi \sigma_i \right) = L_0\left(\tfrac{1}{2} I\right)$$

This says that L would never reveal any information about the input state, violating the hypothesis that L defeats the qubit hiding scheme.

Defeating the cbit hiding

Conclusion from previous slide: there is a k such that $L_0 \neq L_k$



$$\left(L \otimes I_{B_3}\right)\left(\rho_i^{AB_1} \otimes \Phi_+^{B_2B_3}\right) = \left(L_i \otimes I_{B_3}\right)\left(\Phi_+^{B_2B_3}\right)$$

The attack: 1) Bob prepares a local maximally entangled state on B_2B_3

2) Alice and Bob apply L to AB_1B_2

3) Bob performs a measurement on B_2B_3

By Choi, there is a measurement that can partially distinguish L_0 and L_k

Imperfect hiding

Wish to limit distinguishability through LOCC:

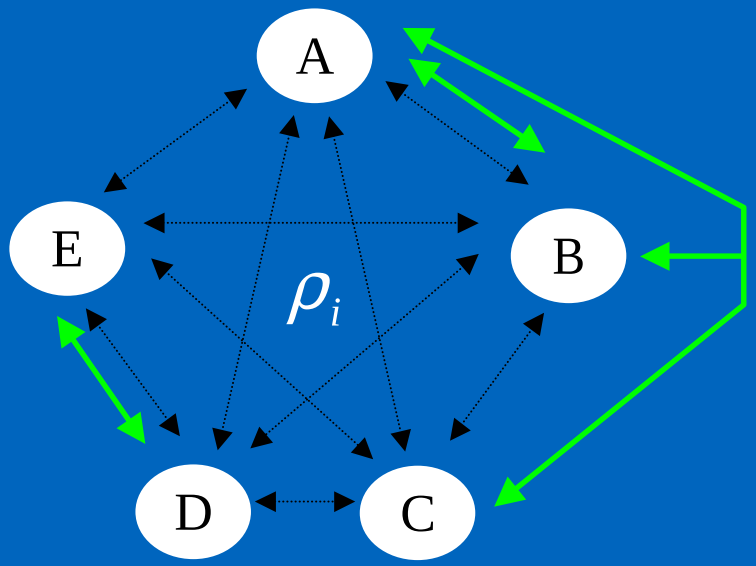
$$\left\| L\left(E\left(\varphi_0\right)\right) - L\left(E\left(\varphi_1\right)\right) \right\|_1 < \varepsilon$$

For all input states and attacks.

If the original 2n bit hiding scheme has security δ, then $\varepsilon < 2^{n+1}\,\delta$.

Not so bad: security of classical hiding schemes *appears* to improve exponentially with number of qubits used.

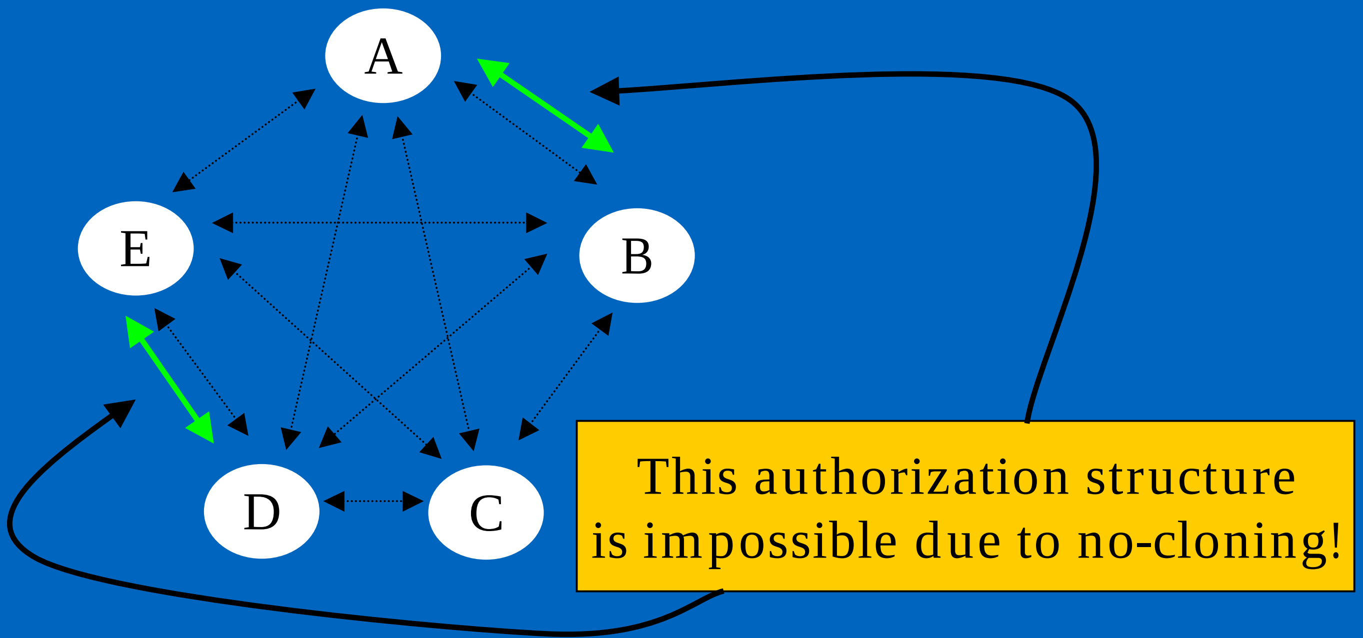
Multipartite cbit hiding



- With LOCC alone the five parties cannot learn *i*
- *Authorized sets* can recover the secret using quantum communication

All monotonic access structures are possible: [Eggeling, Werner 2002]

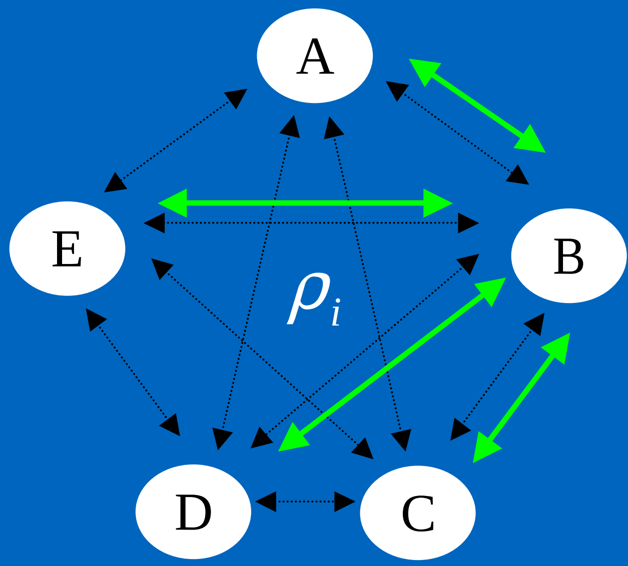
Multipartite qubit hiding



- With LOCC alone the five parties cannot learn φ
- *Authorized sets* can recover the secret using quantum communication

Multipartite qubit hiding

$$E(\varphi) = \frac{1}{4}\sum_{i=0}^{3}$$

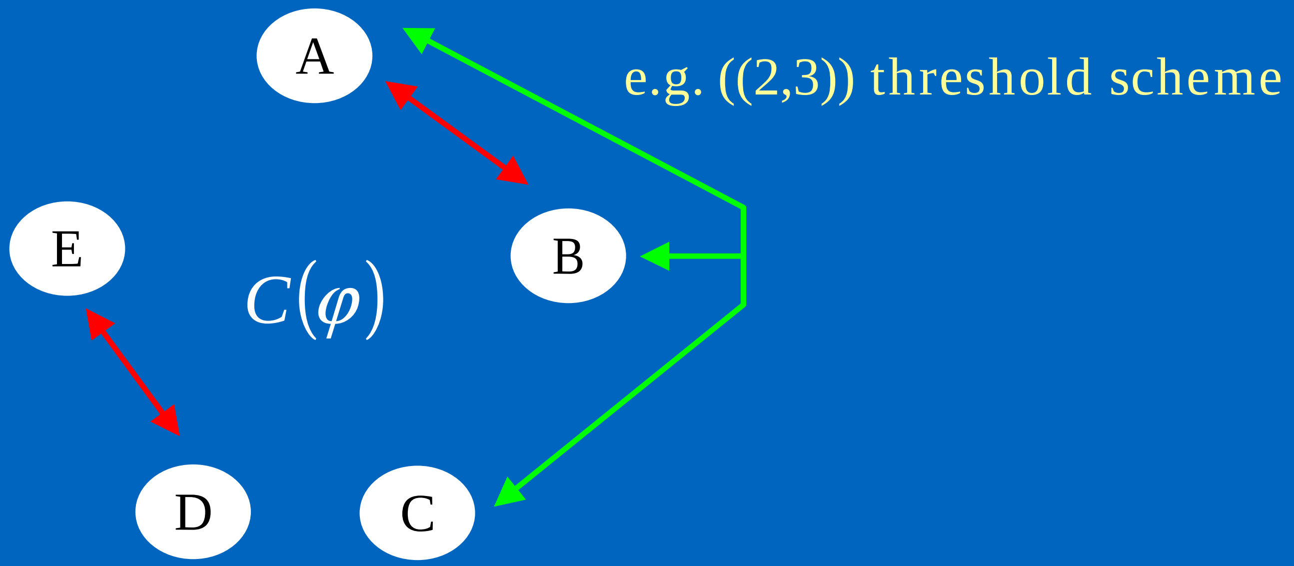


$$\otimes \sigma_i \varphi \sigma_i^{B_2}$$

- With LOCC alone the five parties cannot learn φ
- *Authorized sets* can recover the secret using quantum communication

Problem for generalizing construction: B must be in all authorized sets

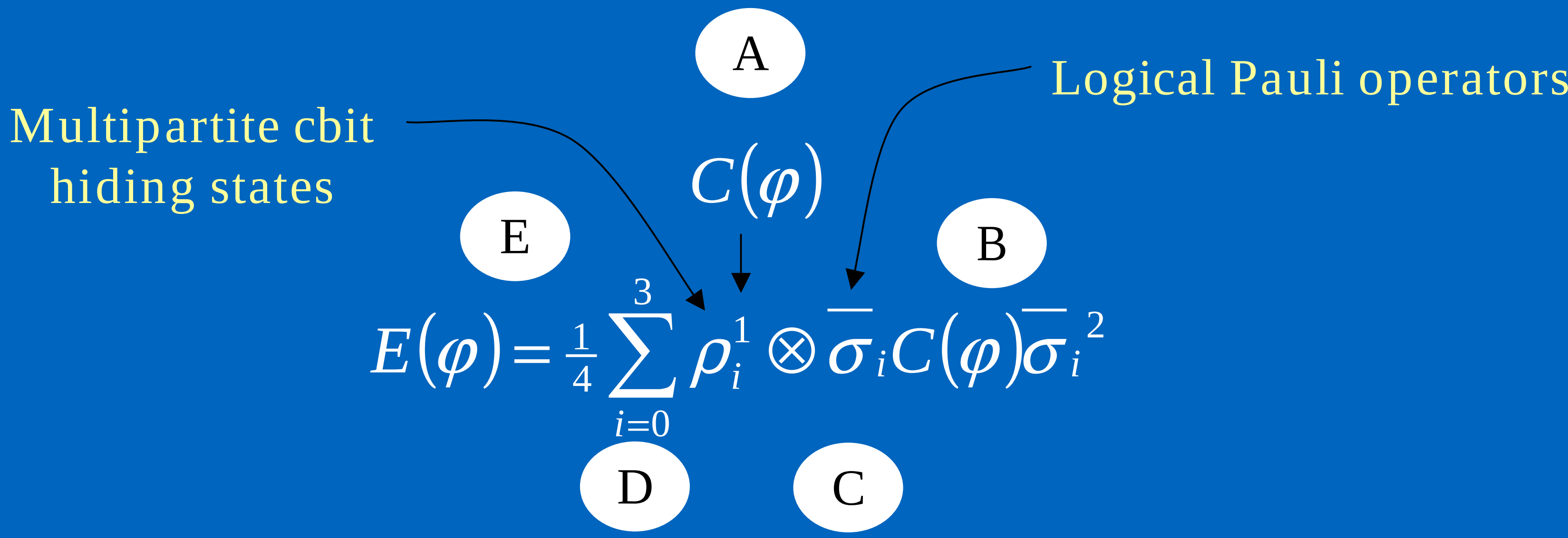
Quantum secret sharing



Secure against quantum communication in unauthorized sets but secret can be recovered by quantum communication in authorized sets.

- ✓All monotonic threshold schemes not violating no-cloning [CGL,1999]
- ✓All monotonic schemes not violating no-cloning [G,2000]

Hiding distributed quantum data



$$C(\varphi)$$

$$E(\varphi) = \frac{1}{4}\sum_{i=0}^{3} \rho_i^1 \otimes \overline{\sigma}_i C(\varphi) \overline{\sigma}_i^{\,2}$$

Resulting state provides strengthening of quantum secret sharing:

- Secure against classical communication between all parties
- Secure against quantum communication in unauthorized sets
- Secret can be recovered only by quantum communication in authorized sets.

✓All monotonic schemes not violating no-cloning

Act II

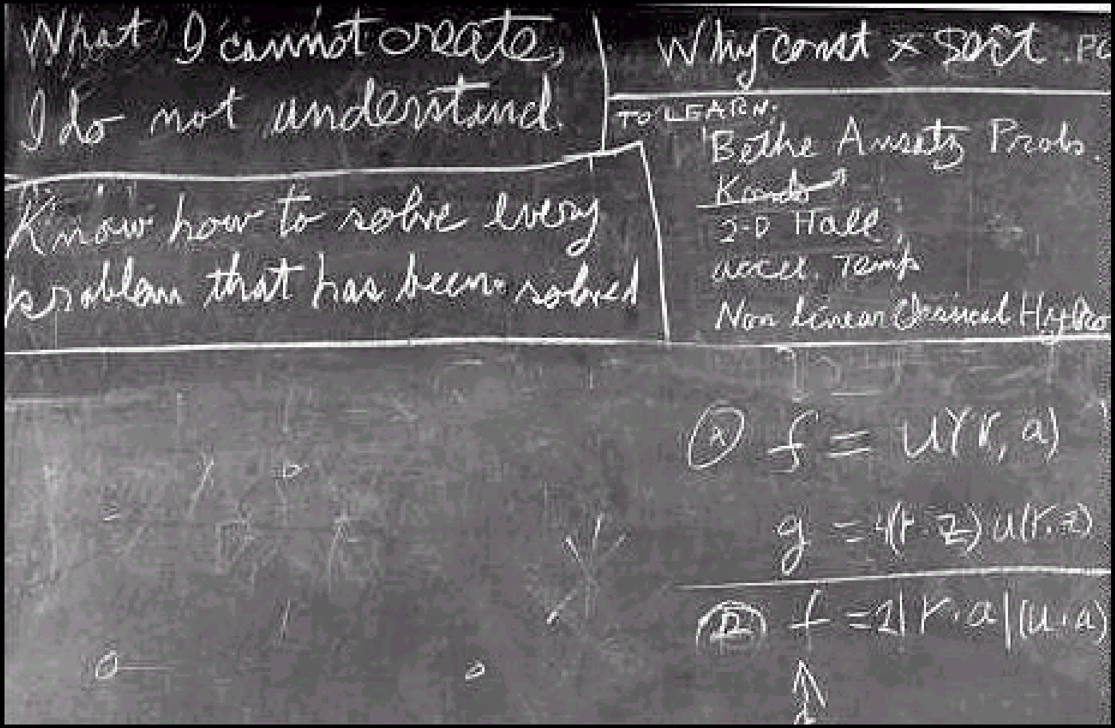
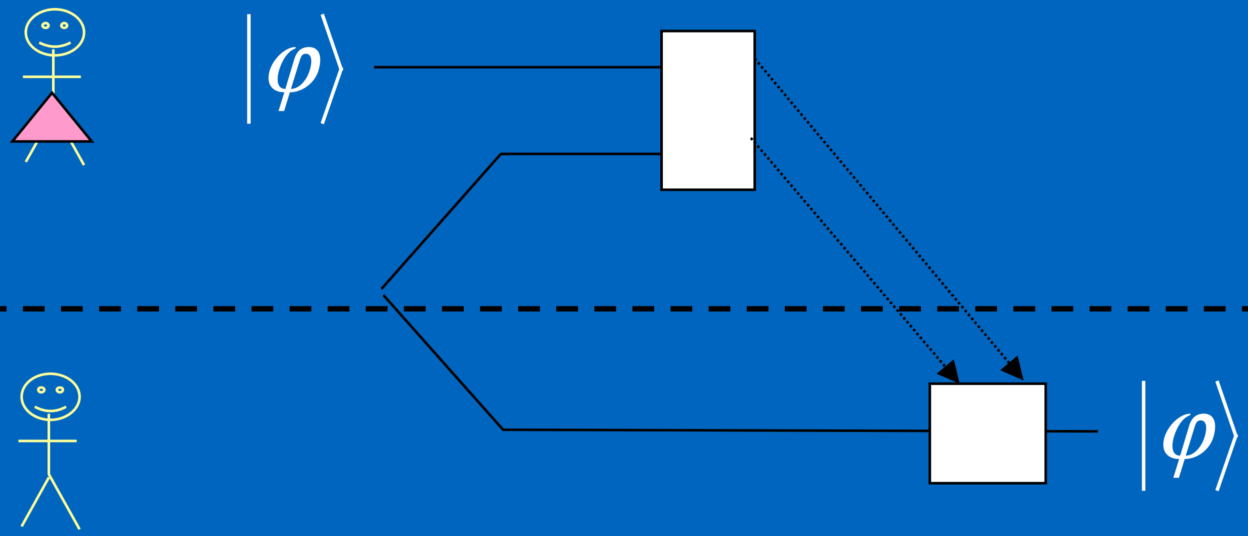


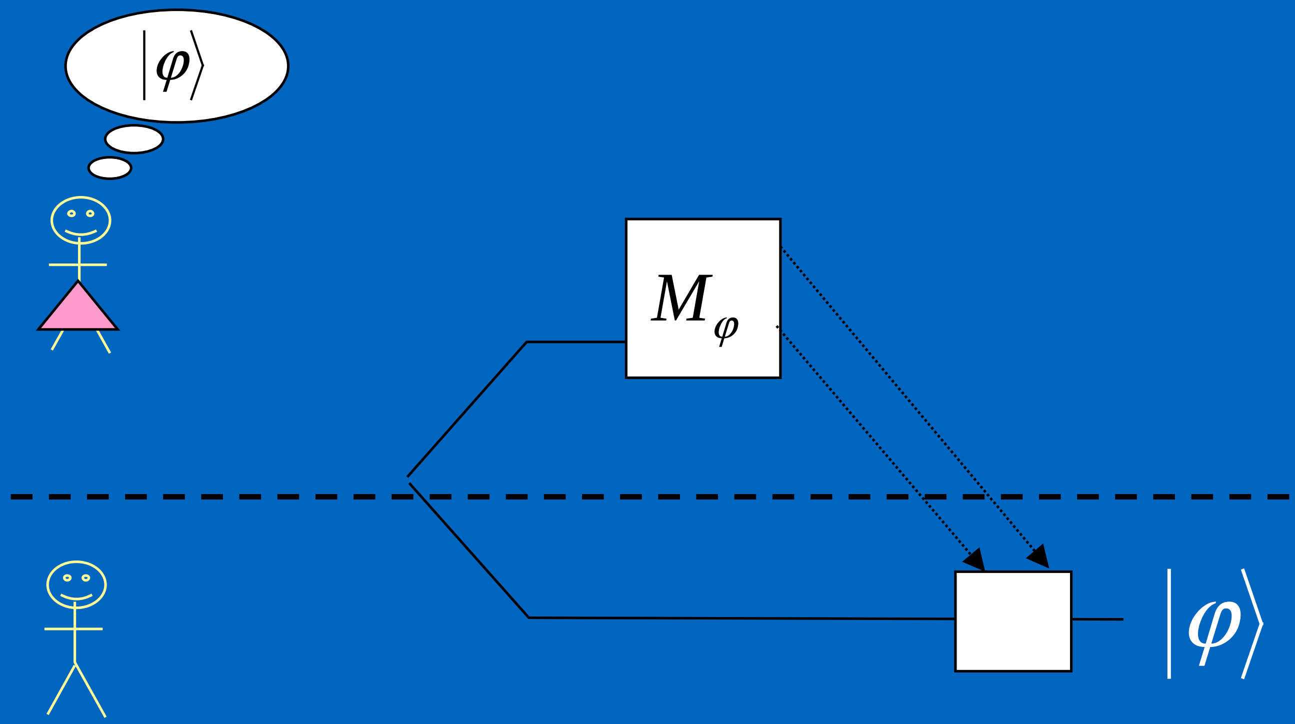
Fig. 1: Glimpse of a master magician’s workshop

Remote state preparation: Non-oblivious teleportation

A circuit that needs no introduction:



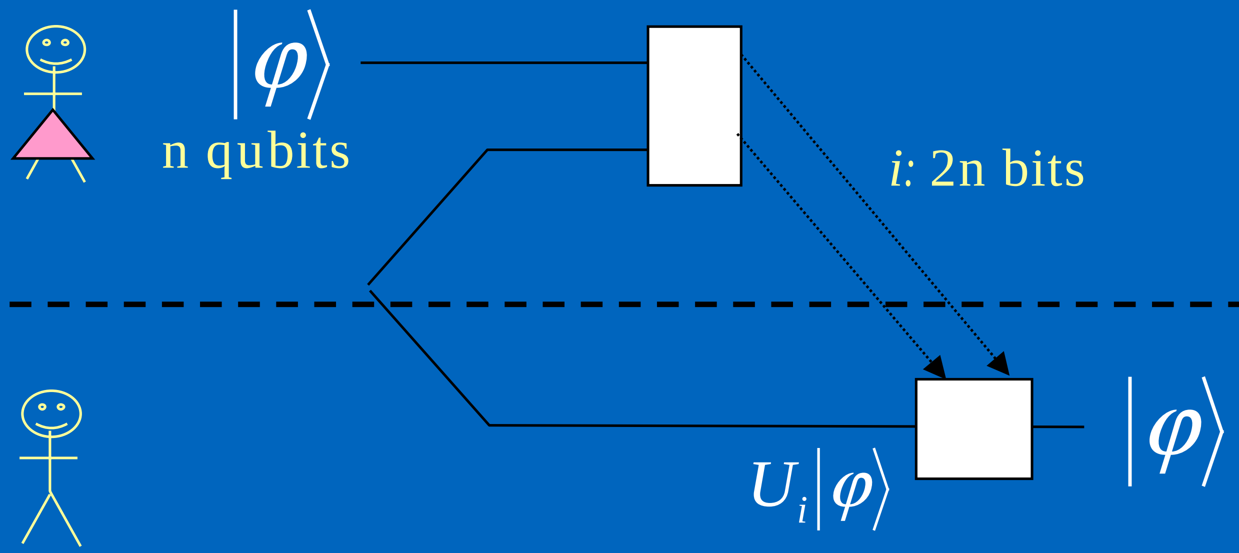
Remote state preparation: Non-oblivious teleportation



Result discussed Sunday: probabilistic, exact RSP of high-dimensional states is possible using 1 ebit + 1 cbit + 1 rbit per qubit.

From RSP to randomization

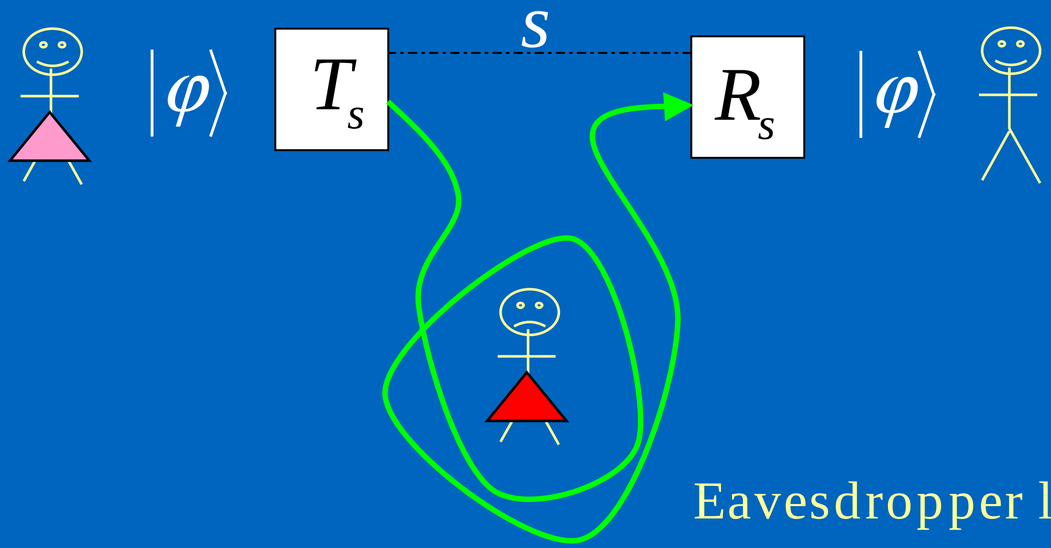
Circuit for teleportation:



Before receiving *i*, Bob knows nothing: $\frac{1}{4^n}\sum_i U_i \varphi U_i^* = \frac{1}{2^n} I$

("Private quantum channel", "Quantum one-time pad", etc.)

Private quantum channels

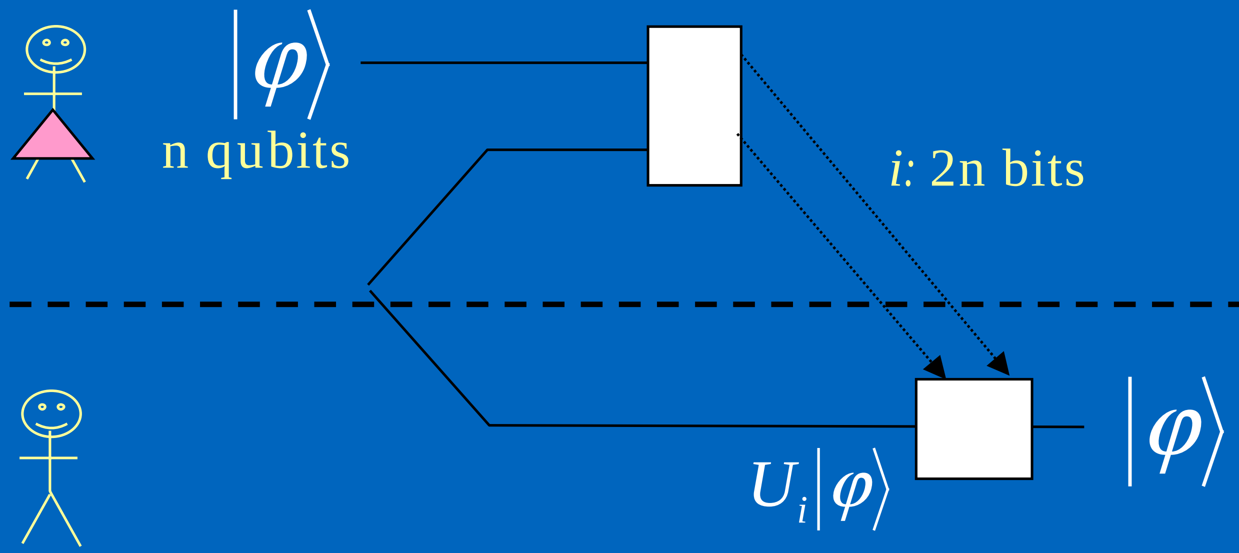


Eavesdropper learns nothing.

[BR,AMTW 2000]

From RSP to randomization

Circuit for teleportation:

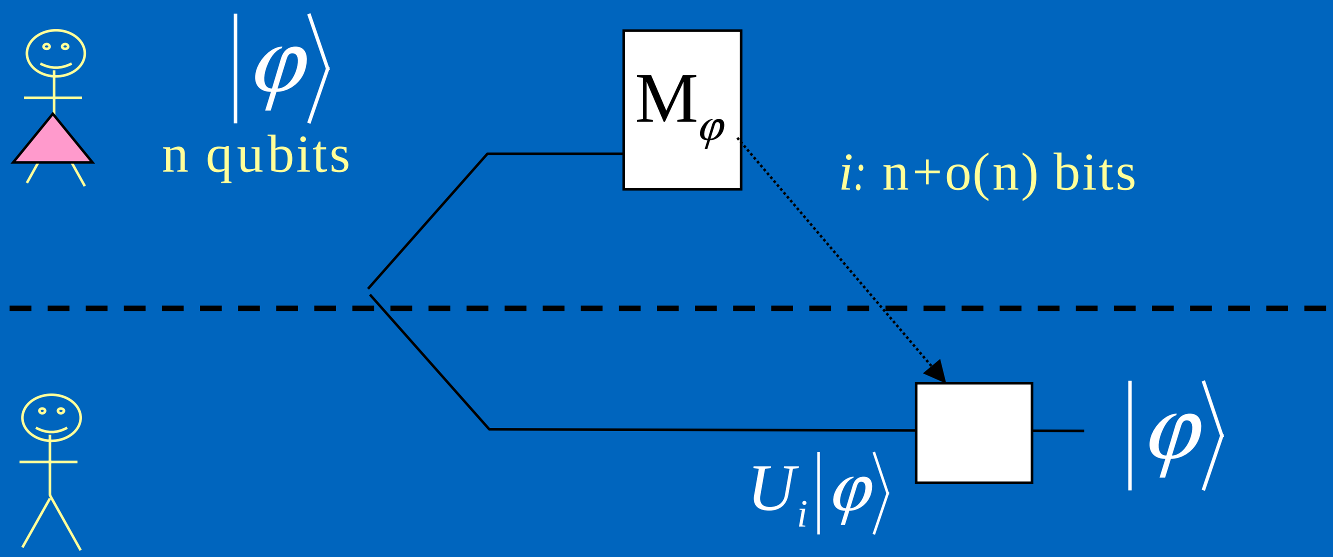


Before receiving i, Bob knows nothing: $\frac{1}{4^n}\sum_i U_i \varphi U_i^* = \frac{1}{2^n} I$

("Private quantum channel", "Quantum one-time pad", etc.)

From RSP to randomization

Circuit for remote state preparation:



Before receiving *i*, Bob knows nothing: $\frac{1}{2^{n+o(n)}}\sum_i U_i \varphi U_i^* \approx \frac{1}{2^n} I$

("Private quantum channel", "Quantum one-time pad", etc.)

On the meaning of "≈"

For any probability density P(φ) on states in C^d and ε>0 there exists a choice of unitaries $\{U_s\}$, $s=1,\ldots,S$ such that

$$\int dP(\varphi) \left\| \frac{1}{S} \sum_{s=1}^{S} U_s \varphi U_s^* - \frac{1}{d} I \right\|_1 < \varepsilon$$

and

$$\log S = \log d + o(\log\log d) + \log\left(\frac{1}{\varepsilon^2}\right)$$

Compare to the perfect private quantum channel:
To achieve ε=0 requires log M = 2 log d.

Another version

There exists a choice of unitaries $\{U_{ps}\}$, $p=1,\ldots,P$, $s=1,\ldots,S$ such that for all states φ in C^d

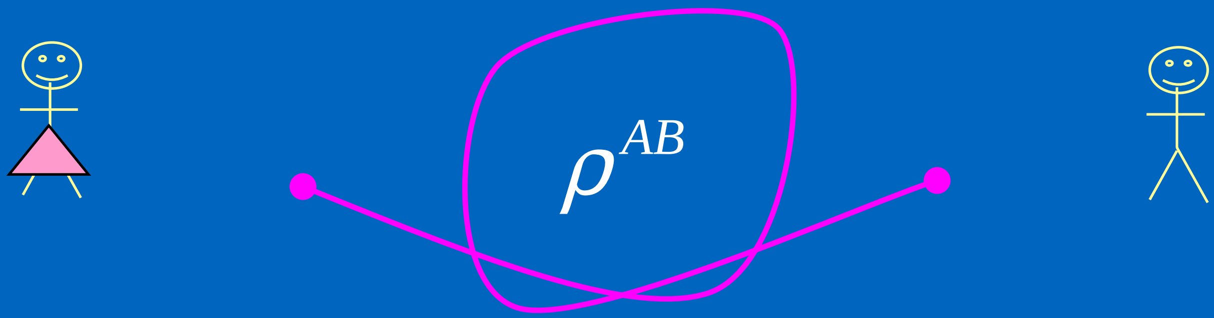
$$\left\| \frac{1}{P}\sum_{p=1}^{P} |p\rangle\langle p| \otimes \frac{1}{S}\sum_{s=1}^{S} U_{ps}\varphi U_{ps}^{*} - \frac{1}{Pd} I \right\|_1 < \varepsilon$$

and

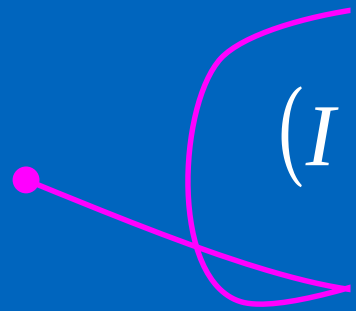
$$\log P = \log S = \log d + o(\log\log d) + \log\left(\frac{1}{\varepsilon^2}\right)$$

Can randomize *every* n-qubit state using 1 secret random bit and 1 public random bit per qubit.

A stronger version of randomization



R is a good randomizer if it destroys all correlations with the outside world:



$$\left(I \otimes R\right)\rho^{AB} \approx \rho^{A} \otimes \tfrac{1}{d} I$$

For separable inputs, this follows from previous formulation.
Not true for entangled inputs!

Rank argument

Recall good randomizing map:

$$T : B\left(C^d\right) \rightarrow B\left(C^P \otimes C^d\right)$$

φ ♋ $\displaystyle \frac{1}{P}\sum_{p=1}^{P} |p\rangle\langle p| \otimes \frac{1}{S}\sum_{s=1}^{S} U_{ps}\varphi U_{ps}^{*}$

Randomizing condition: $\displaystyle T(\varphi) \approx \frac{1}{P} I \otimes \frac{1}{d} I$

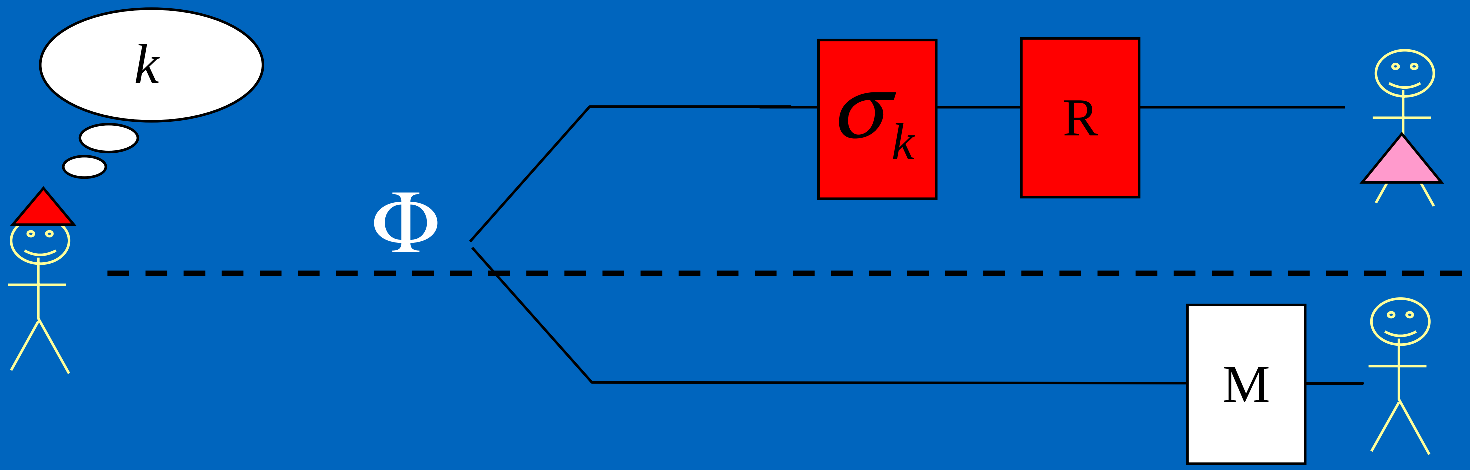
Act on half of a maximally entangled state:

$(T \otimes I)(\Phi_d)$ has rank around $P \cdot d$

Fidelity with maximally mixed state small: $F\left((T \otimes I)\Phi_d, \frac{1}{Pdd} I\right) \lesssim \frac{1}{d}$

Characterizing leftover correlations

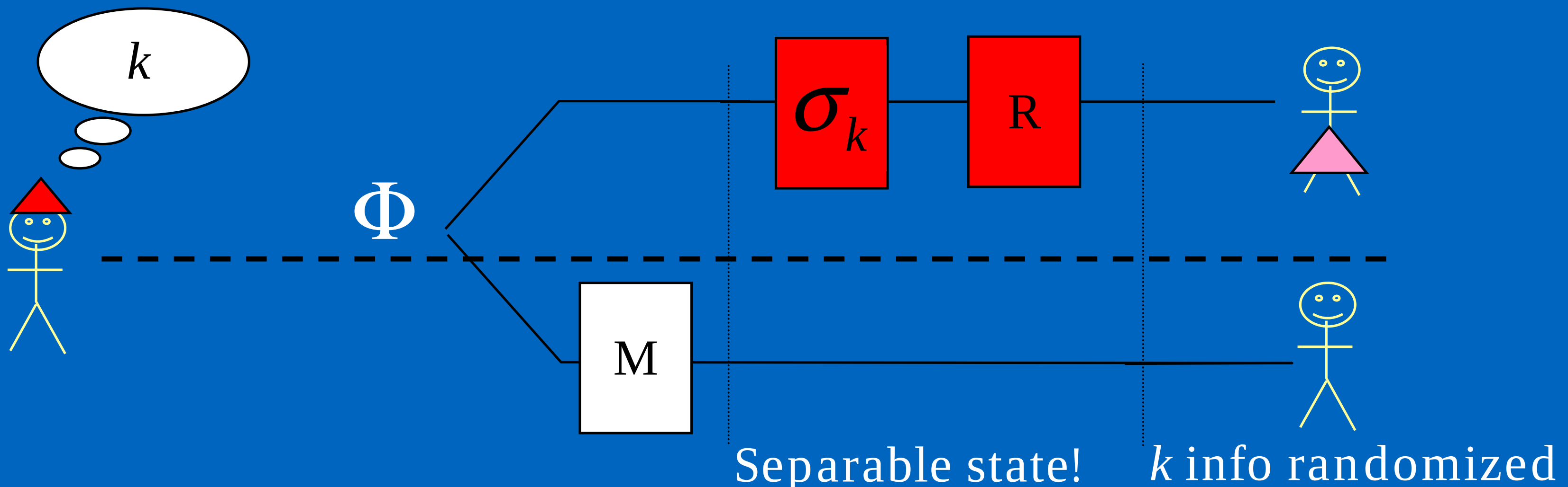
What does randomization map do to entangled inputs?



- Charlie prepares maximally entangled state *k* then randomizes it.
- Bob performs a complete projective measurement.

Characterizing leftover correlations

What does randomization map do to entangled inputs?



- Charlie prepares maximally entangled state *k* then randomizes it.
- Bob performs a complete projective measurement.

Conclusion: the randomizing map is secure against 1-way LOCC

(Highly optimistic) Conjecture

Can randomize *every* n-qubit state using 1 secret random bit per qubit and *no public random bits*.

Given ε>0, there exists a choice of unitaries $\{U_s\}$, $s=1,\ldots,S$ such that for all states φ in C^d

$$\frac{1}{S}\sum_{s=1}^{S} U_s \varphi U_s^* \in \left[\frac{1-\varepsilon}{d} I, \frac{1+\varepsilon}{d} I\right]$$

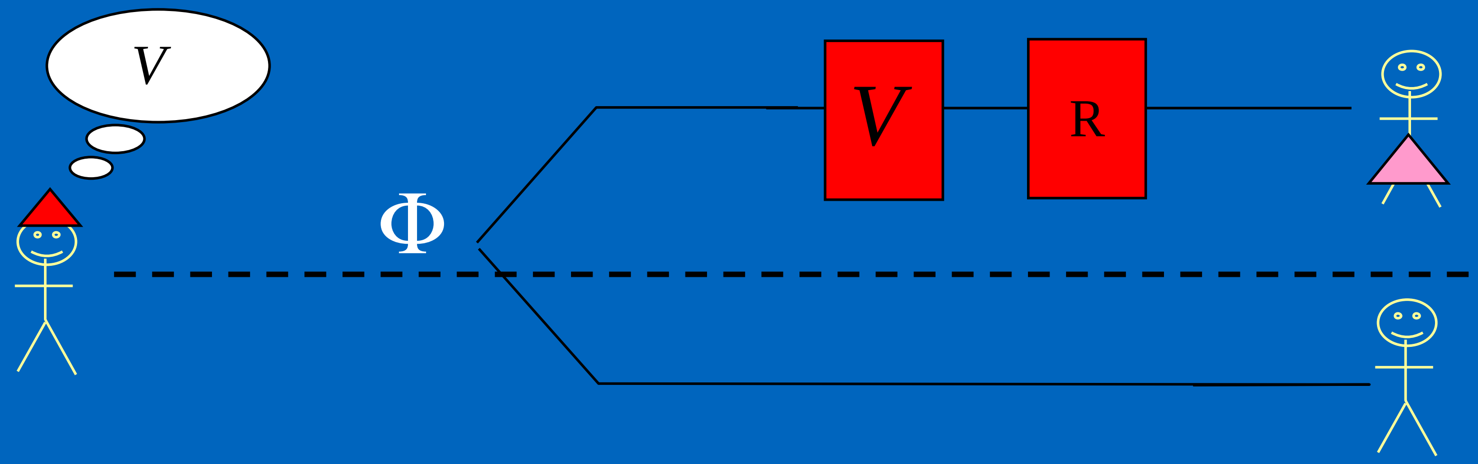
and

$$\log S = \log d + o(\log d) + \log\left(\frac{1}{\varepsilon^2}\right)$$

Consequences

- Universal remote state preparation with only 1 ebit + 1 cbit per qubit
  - (No shared random bits necessary)
- Weakly randomized maximally entangled states indistinguishable from maximally mixed states using LOCC
  - (Not just 1-way LOCC as sketched earlier)

Application to data hiding



Consider ensemble of randomized states with *V* chosen using Haar measure

$$\chi = \log(d^2) - \int dV S((RV \otimes I)\Phi)$$

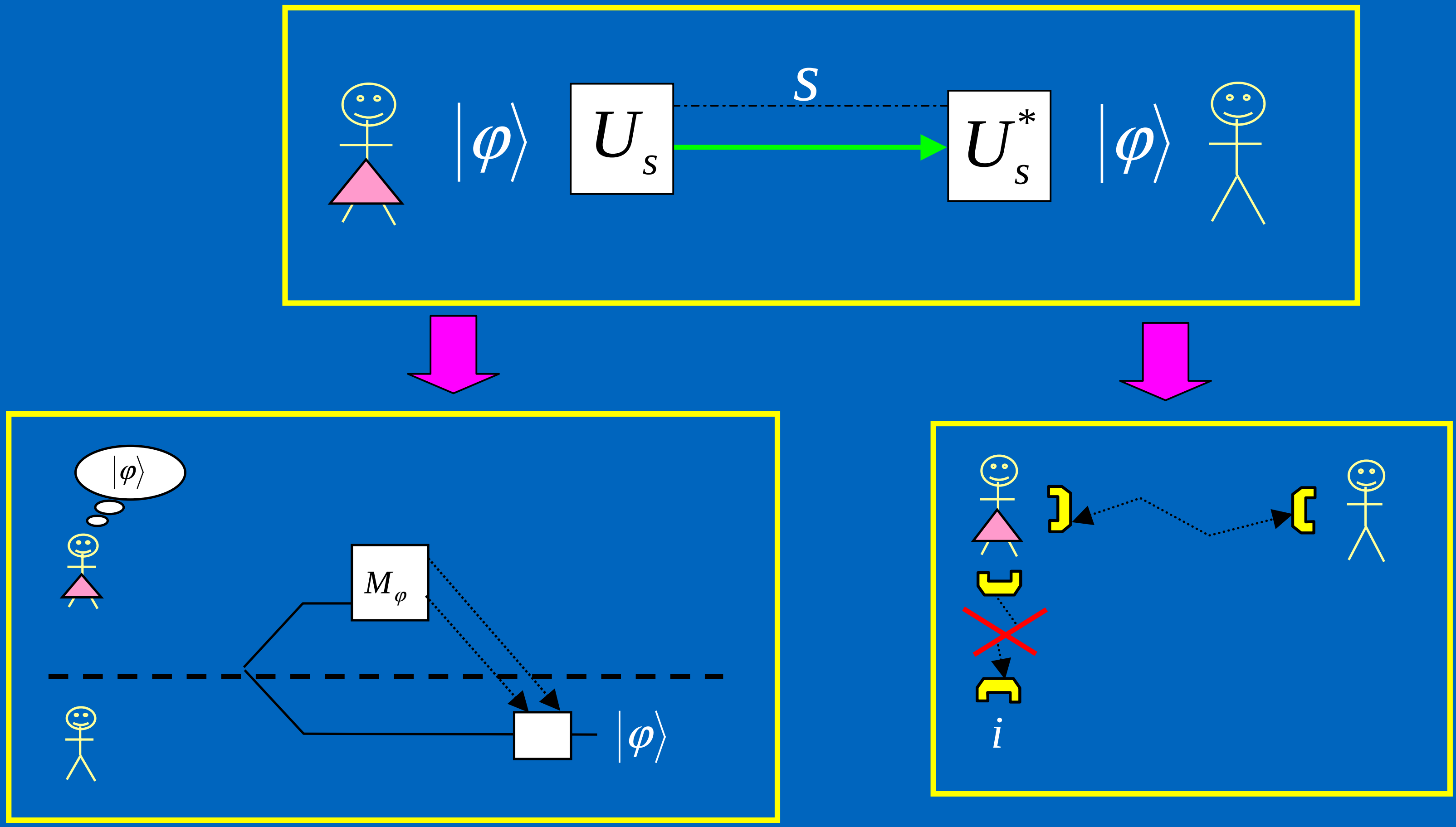
$$\geq \log(d^2) - \log M$$

Rank bound on entropy

$$= \log d - o(\log d) - \log\left(\tfrac{1}{\varepsilon^2}\right)$$

So we can do coding to get about n hidden bits using nxn bipartite states!

Glyph collection



Competing visions

- Faction 1
- Destroying classical correlations requires only 1 rbit per qubit
- Destroying quantum correlations requires 2 rbits per qubit

- Faction 2
- Randomizing an arbitrary pure quantum state requires 1 public rbit and 1 secret rbit per qubit

Summary

- Described a method for hiding qubits given one for hiding bits (construction and proof not restricted to data hiding)
- Outlined a connection between LOCC data hiding, private quantum channels and remote state preparation