Uses of Entanglement (Preskill ch. 4)

Information in entangled Qubit pairs

2 spins ⇨ $\mathcal{D}im(\mathcal{E}=\mathcal{E}_A\otimes\mathcal{E}_B)$ 2 bits of information

* We can store this info in product states
  ⇨ the info is locally available to Alice & Bob

* Alternatively, we can store this info in EPR basis

$$|\Phi^\pm\rangle = \frac{1}{\sqrt{2}}(|\uparrow\uparrow\rangle \pm |\downarrow\downarrow\rangle)$$
$$|\Psi^\pm\rangle = \frac{1}{\sqrt{2}}(|\uparrow\downarrow\rangle \pm |\downarrow\uparrow\rangle)$$

} maximally entangled states

Parity bit ($|\Phi\rangle$ or $|\Psi\rangle$)

Phase bit ("+" or "−")

} not locally accessible to Alice & Bob

* Perhaps surprisingly, info stored in the EPR basis can be manipulated locally:

Alice applies σ_x to spin A ⇨ flips $|\uparrow_A\rangle \leftrightarrow |\downarrow_A\rangle$

⇨ $\begin{cases} |\Phi^+\rangle \leftrightarrow |\Psi^+\rangle \\ |\Phi^-\rangle \leftrightarrow -|\Psi^-\rangle \end{cases}$

* Local Unitary U can change any max entangled Bell state to any other!

* Global Unitary U (e. g., CNOT) needed to change entangled states to product states and vice versa

Uses of Entanglement (Preskill ch. 4)

Information in entangled Qubit pairs

2 spins ➡ $\mathcal{D}im(\mathcal{E} = \mathcal{E}_A \otimes \mathcal{E}_B)$ 2 bits of information

* We can store this info in product states
  ➡ the info is locally available to Alice & Bob

* Alternatively, we can store this info in EPR basis

$$|\Phi^\pm\rangle = \frac{1}{\sqrt{2}}(|\uparrow\uparrow\rangle \pm |\downarrow\downarrow\rangle)$$
$$|\Psi^\pm\rangle = \frac{1}{\sqrt{2}}(|\uparrow\downarrow\rangle \pm |\downarrow\uparrow\rangle)$$

} maximally entangled states

Parity bit ($|\Phi\rangle$ or $|\Psi\rangle$)
Phase bit ("+" or "−")

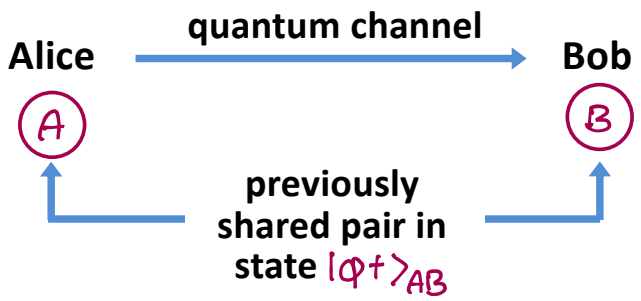
} not locally accessible to Alice & Bob

* Perhaps surprisingly, info stored in the EPR basis can be manipulated locally:

Alice applies σ_x to spin A ➡ flips $|\uparrow_A\rangle \leftrightarrow |\downarrow_A\rangle$

➡ $\begin{cases} |\Phi^+\rangle \leftrightarrow |\Psi^+\rangle \\ |\Phi^-\rangle \leftrightarrow -|\Psi^-\rangle \end{cases}$

Quantum Dense Coding



Basic resource - shared Bell states

$$|\Phi^\pm\rangle = \frac{1}{\sqrt{2}}(|\uparrow\uparrow\rangle \pm |\downarrow\downarrow\rangle)$$
$$|\Psi^\pm\rangle = \frac{1}{\sqrt{2}}(|\uparrow\downarrow\rangle - |\downarrow\uparrow\rangle)$$

Protocol:

(1) Alice applies one of 4 local unitaries

$U = \mathbb{1}$: $|\Phi^+\rangle_{AB} \to |\Phi^+\rangle_{AB}$ $\quad$ $U = \sigma_y$: $|\Phi^+\rangle_{AB} \to |\Phi^-\rangle_{AB}$

$U = \sigma_x$: $|\Phi^+\rangle_{AB} \to |\Psi^+\rangle_{AB}$ $\quad$ $U = \sigma_z$: $|\Phi^+\rangle_{AB} \to |\Phi^-\rangle_{AB}$

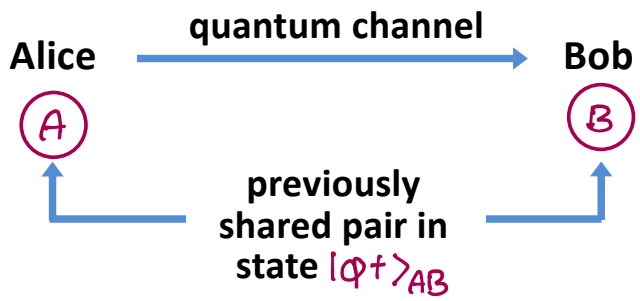
(2) Alice sends (A) to Bob over the quantum channel

(3) Bob does measurement on (AB) that distinguishes the 4 Bell states ➡ Bob receives 2 classical bits of information.

* Proof of principle: entanglement is a resource for communication

Uses of Entanglement (Preskill ch. 4)

Quantum Dense Coding



Basic resource - shared Bell states

$$|\Phi^\pm\rangle = \frac{1}{\sqrt{2}}(|\uparrow\uparrow\rangle \pm |\downarrow\downarrow\rangle)$$
$$|\Psi^\pm\rangle = \frac{1}{\sqrt{2}}(|\uparrow\downarrow\rangle - |\downarrow\uparrow\rangle)$$

Protocol:

(1) Alice applies one of 4 local unitaries

$U = \mathbb{1}$: $|\Phi^+\rangle_{AB} \to |\Phi^+\rangle_{AB}$ $\quad$ $U = \sigma_y$: $|\Phi^+\rangle_{AB} \to |\Psi^-\rangle_{AB}$

$U = \sigma_x$: $|\Phi^+\rangle_{AB} \to |\Psi^+\rangle_{AB}$ $\quad$ $U = \sigma_z$: $|\Phi^+\rangle_{AB} \to |\Phi^-\rangle_{AB}$

(2) Alice sends (A) to Bob over the quantum channel

(3) Bob does measurement on (AB) that distinguishes the 4 Bell states → Bob receives 2 classical bits of information.

* Proof of principle: entanglement is a resource for communication

Note: It is really hard to store entangled qubits

Alice & Bob must probably use channel immediately beforehand ⇨ no obvious gain

But: The message is unconditionally secure, an eavesdropper learns nothing from intercepting Alice's qubit in transmission

Quantum Key Distribution

Provably secure coding scheme: Private key (shared random bit string)

Example:

message → ⊕ key → encrypted → ⊕ key

10100110 $\quad$ 11010111 $\quad$ 01110001 $\quad$ 10100110

info entirely in message/key correlations

Uses of Entanglement (Preskill ch. 4)

Quantum Key Distribution

Alice → (secure message) → Bob

Provably secure coding scheme: Private key (shared random bit string)

Example:

message → ⊕ key → encrypted → ⊕ key

10100110 → 11010111 → 01110001 → 10100110

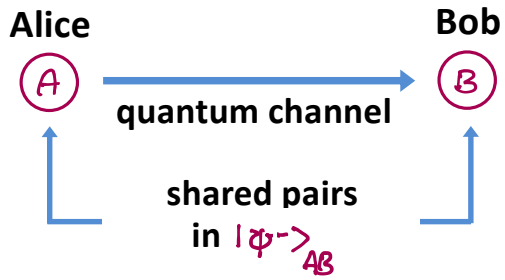
info entirely in message/key correlations

Key Challenge of cryptography: Secure key distribution

Conventional methods

* Exchange by courier ← inconvenient, 3rd party not secure
* Public Key (RSA) ← not provably secure

Idea: Rely on QM for security



Singlet

$|\psi^-\rangle = \frac{1}{\sqrt{2}}(|\uparrow\downarrow\rangle - |\downarrow\uparrow\rangle)$

Bell state

Protocol:

(1) Alice & Bob each measure σ_x or σ_y at random

(2) Alice & Bob exchange classical info on measurement bases, discard pairs when bases where different

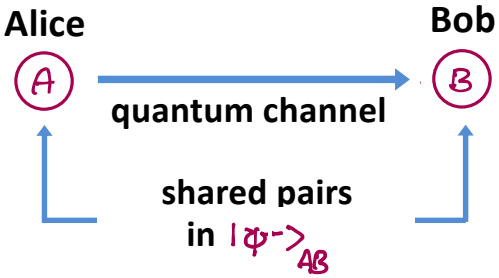
⇨ Remaining qubits are perfectly correlated (private key)

What about eavesdropping?

Can Eve gain access to key? – not by intercepting individual qubits

Uses of Entanglement (Preskill ch. 4)

Idea: Rely on QM for security



Singlet

$|\psi^-\rangle = \frac{1}{\sqrt{2}}(|\uparrow\downarrow\rangle - |\downarrow\uparrow\rangle)$

Bell state

Protocol:

(1) Alice & Bob each measure σ_x or σ_y at random

(2) Alice & Bob exchange classical info on measurement bases, discard pairs when bases where different

➡ Remaining qubits are perfectly correlated (private key)

What about eavesdropping?

Can Eve gain access to key? – not by intercepting individual qubits

What if Eve had access to pairs in the past, and entangled her own qubits with the (AB) pairs such that

$$|\psi^-\rangle_{AB}\,|e\rangle_E \to |\gamma\rangle_{ABE}$$

e. g., $\frac{1}{\sqrt{2}}(|\uparrow\downarrow\rangle_{AB} - |\downarrow\uparrow\rangle_{AB})|0\rangle_e \to \frac{1}{\sqrt{2}}(|\uparrow\downarrow\rangle_{AB}|0\rangle_e - |\downarrow\uparrow\rangle_{AB}|1\rangle_e)$

Security: the state $|\psi^-\rangle_{AB}$ is an eigenstate of Alice & Bob's joint measurements,

$$\sigma_x^{(A)}\sigma_x^{(B)}|\psi^-\rangle_{AB} = \sigma_z^{(A)}\sigma_z^{(B)}|\psi^-\rangle_{AB} = -1\,|\psi^-\rangle_{AB}$$

When Alice & Bob measure $\sigma_x^{(A)}\sigma_x^{(B)}$, $\sigma_z^{(A)}\sigma_z^{(B)}$ and compare, their outcomes must be perfectly (anti) correlated, but entanglement w/Eve's qubit will cause this to occasionally fail.

By publicly sharing (sacrificing) part of their key they can thus detect Eve's presence unless

$$|\gamma\rangle_{ABE} = |\psi^-\rangle_{AB}\,|e\rangle_E$$

What could possibly go wrong?

Uses of Entanglement (Preskill ch. 4)

What if Eve had access to pairs in the past, and entangled her own qubits with the (AB) pairs such that

$$|\psi^-\rangle_{AB}\,|e\rangle_E \to |\gamma\rangle_{ABE}$$

e. g., $\frac{1}{\sqrt{2}}\left(|\uparrow\downarrow\rangle_{AB} - |\downarrow\uparrow\rangle_{AB}\right)|0\rangle_E \to \frac{1}{\sqrt{2}}\left(|\uparrow\downarrow\rangle_{AB}|0\rangle_E - |\downarrow\uparrow\rangle_{AB}|1\rangle_E\right)$

Security: the state $|\psi^-\rangle_{AB}$ is an eigenstate of Alice & Bob's joint measurements,

$$\sigma_x^{(A)}\sigma_x^{(B)}|\psi^-\rangle_{AB} = \sigma_z^{(A)}\sigma_z^{(B)}|\psi^-\rangle_{AB} = -1\,|\psi^-\rangle_{AB}$$

When Alice & Bob measure $\sigma_x^{(A)}\sigma_x^{(B)}$, $\sigma_z^{(A)}\sigma_z^{(B)}$ and compare, their outcomes must be perfectly (anti) correlated, but entanglement w/Eve's qubit will cause this to occasionally fail.

By publicly sharing (sacrificing) part of their key they can thus detect Eve's presence unless

$$|\gamma\rangle_{ABE} = |\psi^-\rangle_{AB}\,|e\rangle_E$$

What could possibly go wrong?

What about errors in the channel ?

* Alice & Bob can do classical error correction on their key bit string
* Errors make it harder to detect an evesdropper
* Privacy amplification: 1 key bit = parity of *n* bits

Note: Entangled pairs are not required for QKD Alice can prepare qubits in one of the 4 states $|\uparrow_x\rangle, |\downarrow_x\rangle, |\uparrow_z\rangle, |\downarrow_z\rangle$ at random, send to Bob who measures σ_x, σ_z at random. They compare preparation/measurement choices, keep the bits where they made the same choices ⇨ private key

This is the Bennet & Brassard (BB-84 Protocol)

Note: QKD systems based on photon polarization and running in fibers or free space have been available for many years. QKD has also been implemented with satellite relays.

npj | Quantum Information

www.nature.com/npjqi

ARTICLE OPEN

Check for updates

Finite key effects in satellite quantum key distribution

Jasminder S. Sidhu[1,2]✉, Thomas Brougham[1,2], Duncan McArthur[1], Roberto G. Pousa[1] and Daniel K. L. Oi[1]✉

Global quantum communications will enable long-distance secure data transfer, networked distributed quantum information processing, and other entanglement-enabled technologies. Satellite quantum communication overcomes optical fibre range limitations, with the first realisations of satellite quantum key distribution (SatQKD) being rapidly developed. However, limited transmission times between satellite and ground station severely constrains the amount of secret key due to finite-block size effects. Here, we analyse these effects and the implications for system design and operation, utilising published results from the Micius satellite to construct an empirically-derived channel and system model for a trusted-node downlink employing efficient Bennett-Brassard 1984 (BB84) weak coherent pulse decoy states with optimised parameters. We quantify practical SatQKD performance limits and examine the effects of link efficiency, background light, source quality, and overpass geometries to estimate long-term key generation capacity. Our results may guide design and analysis of future missions, and establish performance benchmarks for both sources and detectors.

npj Quantum Information (2022)8:18 ; https://doi.org/10.1038/s41534-022-00525-3

INTRODUCTION

Quantum technologies have the potential to enhance the capability of many applications[1] such as sensing[2–4], communications[5–8], and computation[9]. Ultimately, a worldwide networked infrastructure of dedicated quantum technologies, i.e. a quantum internet[10], could enable distributed quantum sensors[11–14], precise timing and navigation[15–17], and faster data processing through distributed quantum computing[18]. This will require the establishment of long distance quantum links at global scale. A fundamental difficulty is exponential loss in optical fibres, which limits direct transmission of quantum photonic signals to < 1000 km[19–22]. Quantum repeaters may overcome the direct transmission limit but stringent performance requirements render them impractical by themselves for scaling to the intercontinental ranges needed for global scale-up[23]. Alternatively, satellite-based free-space transmission significantly reduces the number of ground quantum repeaters required[24].

the secret key rate[37,38]. Analyses based on smooth entropies[32] improve finite-key bounds[39] and have been applied to free-space quantum communication experiments[40]. Recently, tight bounds[36] and small block analyses[41] further improve key lengths for finite signals. Here, we provide a detailed analysis of SatQKD secret key generation, which utilises tight finite block statistics in conjunction with system design and operational considerations.

As part of our modelling, we implement tight statistical analyses for parameter estimation and error correction to determine the optimised, finite-block, single-pass secret key length (SKL) for weak coherent pulse (WCP) efficient BB84 protocols using three signal intensities (two-decoy states). We base our nominal system model on recent experimental results reported by the Micius satellite[42] and use a simple scaling method to extrapolate performance to other SatQKD configurations. The effects of different system parameters are explored, such as varying system link efficiencies, protocol choice, background counts, source quality, and overpass geometries.

Uses of Entanglement (Preskill ch. 4)

What about errors in the channel ?

* **Alice & Bob can do classical error correction on their key bit string**
* **Errors make it harder to detect an evesdropper**
* **Privacy amplification: 1 key bit = parity of *n* bits**

Note: Entangled pairs are not required for QKD
Alice can prepare qubits in one of the 4 states $|\uparrow_x\rangle, |\downarrow_x\rangle, |\uparrow_z\rangle, |\downarrow_z\rangle$ at random, send to Bob who measures σ_x, σ_z at random. They compare preparation/measurement choices, keep the bits where they made the same choices

This is the Bennet & Brassard (BB-84 Protocol)

Note: QKD systems based on photon polarization and running in fibers or free space have been available for many years. QKD has also been implemented with satellite relays.

Aside – No Cloning: Insures against obvious attacks

Let $|\varphi\rangle, |\psi\rangle$ be non-orthogonal states in $\mathcal{E}$
Consider a unitary U that implements the map

$$U: |\varphi\rangle \otimes |0\rangle_E \rightarrow |\varphi\rangle \otimes |e\rangle_E$$
$$U: |\psi\rangle \otimes |0\rangle_E \rightarrow |\psi\rangle \otimes |f\rangle_E$$

Unitarity implies conservation of scalar products

$$\langle\psi|\varphi\rangle = ({}_E\langle 0| \otimes \langle\psi|)(|\varphi\rangle \otimes |0\rangle_E)$$
$$= ({}_E\langle f| \otimes \langle\psi|)(|\varphi\rangle \otimes |e\rangle_E)$$
$$= \langle\psi|\varphi\rangle {}_E\langle f|e\rangle_E$$

Then $\langle\psi|\varphi\rangle \neq 0 \rightarrow {}_E\langle e|f\rangle_E = 1 \rightarrow |e\rangle_E = |f\rangle_E$

Orthogonal states can be copied since $\langle\psi|\varphi\rangle = 0$

Uses of Entanglement (Preskill ch. 4)

Quantum Teleportation

Dense Coding: Quantum info → Send classical info

Teleportation: Classical info → Send quantum info

Scenario: Alice has a qubit in the unknown state $|\psi\rangle_A$

Bob needs this qubit but there is no quantum channel over which to transmit it. What to do?

Idea: Alice measures $\vec{\sigma}^{(A)} \cdot \vec{n}$ → gets $|\uparrow_{\vec{n}}\rangle_A$ or $|\downarrow_{\vec{n}}\rangle_A$

She sends info about the outcome to Bob who use it to prepare $|\uparrow_{\vec{n}}\rangle_B$ or $|\downarrow_{\vec{n}}\rangle_B$ as appropriate. This strategy is not perfect, but we can quantify its performance by calculating the state "fidelity" (probability that Bob has the correct state)

In this case $F = \langle |{}_B\langle\Phi|\psi\rangle_A|^2 \rangle = 2/3$

Random guess $F = {}_A\langle\psi|\rho_B|\psi\rangle_A = 1/2$

Can Alice & Bob do better? Yes!

– they can do "teleportation if they have access to a pair of entangled qubits they shared in the past

Uses of Entanglement (Preskill ch. 4)

Quantum Teleportation

Dense Coding: Quantum info → Send classical info

Teleportation: Classical info → Send quantum info

Scenario: Alice has a qubit in the unknown state $|\psi\rangle_A$

Bob needs this qubit but there is no quantum channel over which to transmit it. What to do?

Idea: Alice measures $\vec{\sigma}^{(A)}\cdot\vec{n}$ → gets $|\uparrow_{\vec{n}}\rangle_A$ or $|\downarrow_{\vec{n}}\rangle_A$

She sends info about the outcome to Bob who use it to prepare $|\uparrow_{\vec{n}}\rangle_B$ or $|\downarrow_{\vec{n}}\rangle_B$ as appropriate. This strategy is not perfect, but we can quantify its performance by calculating the state "fidelity" (probability that Bob has the correct state)

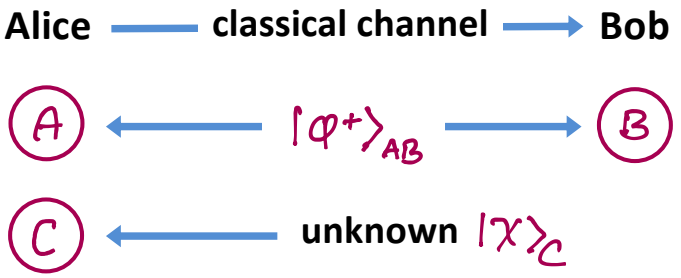
In this case $F = \langle |{}_B\langle\psi|\psi\rangle_A|^2 \rangle = 2/3$

Random guess $F = {}_A\langle\psi|\rho_B|\psi\rangle_A = 1/2$

Can Alice & Bob do better? Yes!

– they can do "teleportation if they have access to a pair of entangled qubits they shared in the past

Teleportation Setup



Reminder: $|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|\uparrow\uparrow\rangle + |\downarrow\downarrow\rangle)$

Protocol:

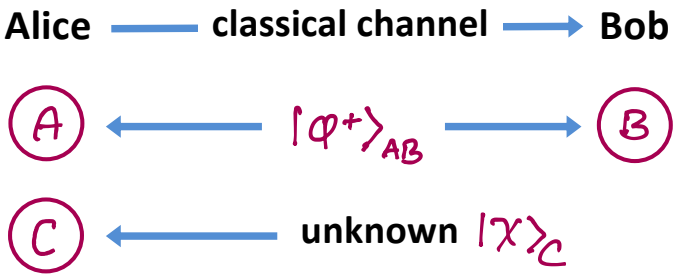
Alice combines (C)(A) and does a 2-qubit measurement in the Bell state basis

- she projects out a state $|\bullet\rangle_{CA}$ which is one of the Bell states $|\Phi^\pm\rangle_{CA}, |\Psi^\pm\rangle_{CA}$

Alice sends classical info to Bob that her actual outcome was the state $|\bullet\rangle_{CA}$

Uses of Entanglement (Preskill ch. 4)

Teleportation Setup



Reminder: $|\varphi^+\rangle = \frac{1}{\sqrt{2}}(|\uparrow\uparrow\rangle + |\downarrow\downarrow\rangle)$

Protocol:

Alice combines (C)(A) and does a 2-qubit measurement in the Bell state basis

- she projects out a state $|\bullet\rangle_{CA}$ which is one of the Bell states $|\phi^\pm\rangle_{CA}, |\psi^\pm\rangle_{CA}$

Alice sends classical info to Bob that her actual outcome was the state $|\bullet\rangle_{CA}$

Bob applies a unitary transformation to (B) according to

if $\|\bullet\rangle_{CA} = \|\varphi^+\rangle_{CA}$	apply	$\mathbb{1}_B$	3-qubit state transforms as
$\|\psi^+\rangle_{CA}$	"	$\sigma_x^{(B)}$	$\|X\rangle_C \otimes \|\varphi^+\rangle_{AB}$
$\|\psi^-\rangle_{CA}$	"	$\sigma_y^{(B)}$	↓
$\|\varphi^-\rangle_{CA}$	"	$\sigma_z^{(B)}$	$\|X\rangle_B \otimes \|\cdot\rangle_{CA}$

Note: At the end Bob's qubit is in the unknown state $|X\rangle$, while Alice's qubit (C) is maximally entangled with (A), i. e., the original state has been completely erased.

Proof: Initial state $|\Psi\rangle_{ABC} = |\varphi^+\rangle_{AB} \otimes (\alpha|\uparrow\rangle_C + \beta|\downarrow\rangle_C)$

Alice's measurement yields, e. g., $|\psi^+\rangle_{AC}$. This projects out the $|\psi^+\rangle_{AC}$ part of $|\Psi\rangle_{ABC}$:

$$P_{AC}|\Psi\rangle_{ABC} = |\psi^+\rangle_{AC}(\alpha|\downarrow\rangle_B + \beta|\uparrow\rangle_B)$$

where $P_{AC} = |\psi^+\rangle_{AC\,AC}\langle\psi^+| \otimes \mathbb{1}_B$

Bob applies $\sigma_x^{(B)}(\alpha|\downarrow\rangle_B + \beta|\uparrow\rangle_B) = (\alpha|\uparrow\rangle_B + \beta|\downarrow\rangle_B) = |X\rangle_B$

Repeat for other Bell state outcomes ➡ QED

Uses of Entanglement (Preskill ch. 4)

Bob applies a unitary transformation to (B) according to

if		apply		3-qubit state transforms as
$\|\Phi\rangle_{CA} = \|\phi^+\rangle_{CA}$		$\mathbb{1}_B$		$\|X\rangle_C \otimes \|\phi^+\rangle_{AB}$
$\|\psi^+\rangle_{CA}$	"	$\sigma_x^{(B)}$		↓
$\|\psi^-\rangle_{CA}$	"	$\sigma_y^{(B)}$		$\|X\rangle_B \otimes \|\cdot\rangle_{CA}$
$\|\phi^-\rangle_{CA}$	"	$\sigma_z^{(B)}$		

Note: At the end Bob's qubit is in the unknown state $|X\rangle$, while Alice's qubit (C) is maximally entangled with (A), i. e., the original state has been completely erased.

Proof: Initial state $|\Phi\rangle_{ABC} = |\phi^+\rangle_{AB} \otimes (\alpha|\uparrow\rangle_C + \beta|\downarrow\rangle_C)$

Alice's measurement yields, e. g., $|\psi^+\rangle_{AC}$ **. This projects out the** $|\psi^+\rangle_{AC}$ **part of** $|\Phi\rangle_{ABC}$**:**

$$P_{AC}|\Phi\rangle_{ABC} = |\psi^+\rangle_{AC}(\alpha|\downarrow\rangle_B + \beta|\uparrow\rangle_B)$$

↑

where $P_{AC} = |\psi^+\rangle_{AC\,AC}\langle\psi^+| \otimes \mathbb{1}_B$

Bob applies $\sigma_x^{(B)}(\alpha|\downarrow\rangle_B + \beta|\uparrow\rangle_B) = (\alpha|\uparrow\rangle_B + \beta|\downarrow\rangle_B) = |X\rangle_B$

Repeat for other Bell state outcomes ➡ QED

Preskill: Show that for any $|\Psi\rangle_{ABC}$ **we have**

$$|\Psi\rangle_{ABC} = \tfrac{1}{2}|\phi^+\rangle_{CA}|X\rangle_B + \tfrac{1}{2}|\psi^+\rangle_{CA}\sigma_x^{(B)}|X\rangle_B + \tfrac{1}{2}|\psi^-\rangle_{CA}(-i\sigma_y^{(B)})|X\rangle_B + \tfrac{1}{2}|\phi^-\rangle_{CA}\sigma_z^{(B)}|X\rangle_B$$

QED !

Discussion:

- **Initially the unknown** $|X\rangle_C$ **is separate from** $|\phi^+\rangle_{AB}$**, qubit C is not entangled with qubits A & B.**
- **Alice's measurement creates correlation between A,C**
- **Alice's outcome is random ➡ no info about** $|X\rangle_C$
- **Info allows Bob to manipulate B to create** $|X\rangle_B$
- **Consistent w/no cloning:** $|X\rangle_C$ **is erased in the measurement that allows Bob to create** $|X\rangle_B$

What might this be good for ?