Few Notations

- We denote $|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ and $|-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$,
- Also, $\ominus = \{|0\rangle, |1\rangle\}$ and $\oslash = \{|+\rangle, |-\rangle\}$ are two orthogonormal bases (rectilinear and diagonal resp.) in $\mathcal{H}_2$,
- The 4 states $\mathbf{BB84} = \{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$ are called the BB84 states,
- $\mathbf{BB84}(0) = \{|0\rangle, |+\rangle\}$ are the two non-orthogonal encoding of classical bit 0,
- $\mathbf{BB84}(1) = \{|1\rangle, |-\rangle\}$ are the two non-orthogonal encoding of classical bit 1.
- $|\gamma_0\rangle = \cos\frac{\pi}{8}|0\rangle + \sin\frac{\pi}{8}|1\rangle$ and $|\gamma_1\rangle = \sin\frac{\pi}{8}|0\rangle - \cos\frac{\pi}{8}|1\rangle$ are states of the Breidbard basis $\{|\gamma_0\rangle, |\gamma_1\rangle\}$.

BRICS

Purification (I)

BB84(0)	**BB84***(0)
1. Alice chooses $b \in_R \{0, +\}$, 2. Alice sends $\|b\rangle$,	1. Alice prepares $$\|S(0)\rangle = \frac{1}{\sqrt{2}}(\|0\rangle_1 \|0\rangle_2 + \|1\rangle_1 \|+\rangle_2)$$ 2. Alice sends particle 2 and keeps particle 1.

The state ρ_2 of particle 2 in **BB84***(0) is

$$\rho_2 = \mathrm{Tr}_1(|S(0)\rangle\langle S(0)|) = \frac{1}{2}(|0\rangle\langle 0| + |+\rangle\langle +|) = \rho_{BB84}(0).$$

- **BB84***(0) is called a purification of **BB84**(0). The purified version does not use any coin.
- In **BB84***(0) Alice does not know the state sent before she measures particle 1.

BRICS

Purification (II)

One could also purify the mixture of pure states $\mathcal{B} = \{(\,|\gamma_0\rangle, \cos^2\frac{\pi}{8}), (\,|\gamma_1\rangle, \sin^2\frac{\pi}{8})\}$ the same way:

$$|\mathcal{B}^*\rangle = \cos\frac{\pi}{8}\,|0\rangle_1\,|\gamma_0\rangle_2 + \sin\frac{\pi}{8}\,|1\rangle_1\,|\gamma_1\rangle_2$$

which satisfies

$$\rho_{\mathcal{B}} = \mathrm{Tr}_1(\,|\mathcal{B}^*\rangle\langle\mathcal{B}^*|) = \cos^2\frac{\pi}{8}\,|\gamma_0\rangle\langle\gamma_0| + \sin^2\frac{\pi}{8}\,|\gamma_1\rangle\langle\gamma_1| = \rho(0).$$

- Nothing can tell given only particle 2 whether it is part of $|B^*\rangle$ or $|S(0)\rangle$.
- One can transform one into the other by applying a transformation to particle 1 alone...

BRICS

Equivalence between Purifications

Let U be the unitary transform acting in a 2-dimensional Hilbert space:

$$|0\rangle \mapsto \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \text{ and } |1\rangle \mapsto \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$$

Let's apply U on the particle 1 of $|S(0)\rangle$,

$$\begin{aligned}(U \otimes \mathbb{1}))|S(0)\rangle &= (U \otimes \mathbb{1})\frac{1}{\sqrt{2}}(|0\rangle_1 |0\rangle_2 + |1\rangle_1 |+\rangle_2) \\ &= \frac{1}{2}((|0\rangle_1 - |1\rangle_1)|0\rangle_2 + (|0\rangle_1 + |1\rangle_1)|+\rangle_2) \\ &= \frac{1}{2}\{|0\rangle_1(|0\rangle + |+\rangle) + |1\rangle(-|0\rangle + |+\rangle)\} \\ &= \cos\frac{\pi}{8}|0\rangle|\gamma_0\rangle + \sin\frac{\pi}{8}|1\rangle|\gamma_1\rangle = |B^*\rangle.\end{aligned}$$

BRICS

HJW Theorem (a special case)

Theorem [HJW93]. *Any pairs of purifications* $\{\,|\Psi_0\rangle,\,|\Psi_1\rangle\}$ *in* $H_1 \otimes H_2$ *for* $\rho \in H_2$ *is related by some unitary transform* $U_{0,1} \in H_1$ *that satisfies:*

$$|\Psi_1\rangle^{1,2} = (U_{0,1} \otimes \mathbf{I}_2)\,|\Psi_0\rangle^{1,2}.$$

Proof: Write $|\Psi_0\rangle$ and $|\Psi_1\rangle$ in the Schmidt form:

$$|\Psi_0\rangle = \sum_{i=1}^{r} \sqrt{\lambda_i} \qquad |e_i^{(0)}\rangle \qquad \otimes |f_i\rangle$$

$$\Updownarrow\; U_{0,1}$$

$$|\Psi_1\rangle = \sum_{i=1}^{r} \sqrt{\lambda_i} \qquad |e_i^{(1)}\rangle \qquad \otimes |f_i\rangle$$

$\lambda_1, \ldots, \lambda_r$ are the eigenvalues of $\rho = \mathrm{Tr}_1(\,|\Psi_0\rangle\langle\Psi_0|) = \mathrm{Tr}_1(\,|\Psi_1\rangle\langle\Psi_1|)$, and $\{\,|e_i^{(b)}\rangle\}_i$ and $\{\,|f_i\rangle\}_i$ are orthonormal bases for $\mathcal{H}_1$ and $\mathcal{H}_2$.

BRICS

Implications

We have seen,

- Purifications allow to encapsulate a quantum mixture in a pure state.
- Different purifications of the same density matrix ρ are related by some unitary transform $U_{0,1}$ that is the identity on $\rho \in H_2$,
- Purifications are therefore all equivalent under local quantum computation,

We shall see,

- Quantum 2-Party protocols can be implemented in such a way that each execution with the same classical inputs generates the same state. This process is called the purification of a quantum protocols,
- This implies that no quantum bit commitment is secure against both parties.

BRICS

Purifying a measurement

1. Alice chooses $\theta \in_R \{\ominus, \oslash\}$,
2. Alice measures photon π in basis θ and gets the outcome $\hat{b}$,
3. Alice announces $\hat{b}$ to Bob.

convention: $|\ominus\rangle = |0\rangle$ and $|\oslash\rangle = |1\rangle$.

Let U_M acting on quantum register $|\bullet\rangle$ and the received qubit $|\bullet\rangle$:

$$\overbrace{\frac{1}{\sqrt{2}}(|\ominus\rangle + |\oslash\rangle)}^{\text{state of the register}} \overbrace{|0\rangle}^{\text{photon } \pi} \mapsto \frac{1}{\sqrt{2}}(|\ominus\rangle|0\rangle + \frac{1}{\sqrt{2}}(|\oslash\rangle|0\rangle + |\oslash\rangle|1\rangle))$$

$$\frac{1}{\sqrt{2}}(|\ominus\rangle + |\oslash\rangle) \quad |1\rangle \mapsto \frac{1}{\sqrt{2}}(|\ominus\rangle|1\rangle + \frac{1}{\sqrt{2}}(|\oslash\rangle|0\rangle - |\oslash\rangle|1\rangle))$$

BRICS

An Example

$$U_M \frac{1}{\sqrt{2}}(|\ominus\rangle + |\oslash\rangle)|+\rangle = U_M \frac{1}{2}(|\ominus\rangle + |\oslash\rangle)(|0\rangle + |1\rangle)$$

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

- The construction can easily be generalized for $\theta \in \{(p, \ominus), (1-p, \oslash)\}$ (for any $0 \leq p \leq 1$) by starting with state

$$\sqrt{p}\,|\ominus\rangle + \sqrt{1-p}\,|\oslash\rangle$$

- Measuring $|\bullet\rangle$ alone gives the classical outcome of an *undetermined* random measurement $\{\ominus, \oslash\}$.

⇒ The outcome $\hat{b}$ can be obtained without θ being determined,

⇒ Purifying a measurement postpones the choice of it until it is really required.

BRICS

Purifying Quantum Protocols (I)

1. Set an internal register with a fresh **random bit** according to distribution $\{(0,p),(1,1-p)\}$,
2. **Compute** a function f of the set of registers and store the outcome,
3. **Send** the content of a quantum register to the peer,
4. **Classical announcement** to the peer of the content of one register,
5. **Quantum reception** of a new qubit,
6. **Classical reception** of a new classical bit.

Purifying Quantum Protocols (II)

1. **Randomness:** A new quantum register $|R\rangle$ is set to

$$|R\rangle = \sqrt{p}\,|0\rangle + \sqrt{1-p}\,|1\rangle.$$

2. **Computation/Measurement:** Let U_f the unitary transformation implementing f and acting on the set $\mathcal{V}$ of registers. The new state $\mathcal{V}'$ for the registers is

$$|\mathcal{V}'\rangle = U_f\,|\mathcal{V}\rangle.$$

3. **Quantum transmission:** A quantum register is sent away.
4. **Classical announcement:** The register containing the bit is measured (in the standard basis $\ominus$) and the classical result announced.
5. **Quantum/Classical reception:** The received qubit is added to the set of registers.

BRICS

Mayers' Theorem (ind. disc. Lo & Chau)

Theorem[PRL97]. Any unconditionally concealing quantum bit commitment protocol is necessarily not binding.

Proof sketch. Assume $\rho_0 = \rho_1$ where ρ_b is the mixed state sent when Alice commits upon b.

Let $|\Psi_0\rangle \in H_A \otimes H_B$ and $|\Psi_1\rangle \in H_A \otimes H_B$ be the purifications for Commit(0) and Commit(1) respectively,

$$\begin{aligned} |\Psi_0\rangle &= \sum_i \lambda_i \, |e_i^{(0)}\rangle \otimes |f_i\rangle \\ |\Psi_1\rangle &= \sum_i \lambda_i \, |e_i^{(1)}\rangle \otimes |f_i\rangle . \end{aligned}$$

since $|\Psi_0\rangle$ and $|\Psi_1\rangle$ are purifications of the same density matrix $\rho = \rho_0 = \rho_1$ (i.e. *required for perfectly concealing commitments*).

BRICS

Cheating Alice

- Alice executes the purification $|\Psi_0\rangle$ for **commit**(0),
- If Alice wants to unveil 0 she just executes **unveil**(0) from $|\Psi_0\rangle$,
- If Alice wants to unveil 1:
  - She applies $U_{0,1} \in H_A$ to her part of $|\Psi_0\rangle$ promised by Theorem [HJW93],

$$|\Psi_1\rangle = (U_{0,1} \otimes \mathbb{1}_B)\, |\Psi_0\rangle,$$

  - She executes **unveil**(1) from $|\Psi_1\rangle$.

⇒ How to generalize to the case where the commitments are *statistically concealing*:

$$\rho_0 \approx \rho_1?$$

BRICS

Statistically Concealing Commitments

If $\Lambda_0 = \{\rho_0^{(n)}\}$ and $\Lambda_1 = \{\rho_1^{(n)}\}$ are statistically indistinguishable,

$$B(\rho_0^{(n)}, \rho_1^{(n)}) \geq 1 - \epsilon^n \Rightarrow$$

$$|\Psi_1\rangle \in \text{Purif}(\rho_1^{(n)}),\ |\hat{\Psi}_1\rangle \in \text{Purif}(\rho_0^{(n)}) : \|\langle \Psi_1 | \hat{\Psi}_1 \rangle\| \geq 1 - \epsilon^n$$

Let $\hat{U}_{0,1}$ be such that $|\hat{\Psi}_1\rangle = (\hat{U}_{0,1} \otimes \mathbb{1}_B)\,|\Psi_0\rangle$ (from [HJW93]):

Alice's Attack

- Alice executes the purification $|\Psi_0\rangle$ for **commit**(0),
- If Alice wants to unveil 0 she just executes **unveil**(0) from $|\Psi_0\rangle$,
- If Alice wants to unveil 1:
  - She applies $\hat{U}_{0,1} \in H_A : |\hat{\Psi}_1\rangle = (\hat{U}_{0,1} \otimes \mathbb{1}_B)\,|\Psi_0\rangle$,
  - She executes **unveil**(1) from $|\hat{\Psi}_1\rangle$.

BRICS