Bit commitment

QKD lets us securely establish a shared key
But there are other cryptographic tasks that this doesn't address
One such task: <u>bit commitment</u>
Turns out to be impossible even in QM! (to get unconditional security)

<u>Problem</u>
Alice wants to commit a bit $b \in \{0,1\}$ to Bob with two properties:
- Binding: A can't change the committed bit
- Concealing: B can't learn the bit until A reveals it

Classical protocol: A writes the bit down, locks it in a safe, gives the safe (but not the key) to B
To reveal, A gives B the key

Problem: not concealing; in principle, B could break open the safe
We really want an info-theoretically secure protocol. Not possible classically.

Could we give a Q protocol?

<u>Ex</u>: Consider the following protocol

Commit phase: let $S_0 = \{|0\rangle, |1\rangle\}$, $S_1 = \{|+\rangle, |-\rangle\}$
A prepares a qubit in a uniformly random state from S_b, sends it to B

Reveal phase: A tells B the value of b & which state was used to encode it
i.e., if $|\phi_{bc}\rangle = H^b|c\rangle$
(so $S_b = \{|\phi_{b0}\rangle, |\phi_{b1}\rangle\}$),
she tells B the bits b, c.
To check, B measures the qubit in the basis S_b.
If he gets $|\phi_{bc}\rangle$, he accepts; otherwise he rejects.

Is this secure?

Clearly the protocol is concealing.

If $b=0$, B sees the density matrix $\frac{1}{2}(|0\rangle\langle 0| + |1\rangle\langle 1|) = I/2$

If $b=1$, B sees the density matrix $\frac{1}{2}(|+\rangle\langle +| + |-\rangle\langle -|) = I/2$

so B cannot learn anything about b.

But it is not binding.

If A prepares her qubit in some pure state, she cannot cheat.

But she can cheat using entanglement.

Suppose she creates $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$, sends one qubit to B.

- To reveal $b=0$, she measures her qubit in the standard basis; call the result c. Then B also has $|c\rangle$.
  She tells him 0c.
- To reveal $b=1$, she measures her qubit in the $|\pm\rangle$ basis.
  Note that $\frac{1}{\sqrt{2}}(|++\rangle + |--\rangle) = \frac{1}{2\sqrt{2}}[(|0\rangle+|1\rangle)(|0\rangle+|1\rangle) + (|0\rangle-|1\rangle)(|0\rangle-|1\rangle)]$
  $= \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$
  So when she gets the $\pm$ outcome, Bob gets $|\pm\rangle$
  So she tells him 10 if she gets + and 11 if she gets −

Since A can reveal either $b=0$ or $b=1$, the protocol is not binding.

General impossibility proof (sketch)

Recall from A4, problem 4d: If $\mathrm{tr}_B|\psi\rangle\langle\psi| = \mathrm{tr}_B|\phi\rangle\langle\phi|$, $\exists$ a unitary on B so that $|\phi\rangle = (I\otimes U)|\psi\rangle$.

Protocol has two phases: commit & reveal

Let the joint state of A&B (pure WLOG) at end of commit phase be $|\psi_b\rangle_{AB}$, depending on A's bit b.

Perfectly concealing: $\mathrm{tr}_A|\psi_0\rangle\langle\psi_0| = \mathrm{tr}_A|\psi_1\rangle\langle\psi_1|$

so $\exists$ a unitary on A so that $(U\otimes I)|\psi_0\rangle = |\psi_1\rangle$,

which means A can cheat — the protocol is not binding.

More generally, one can show that if $\mathrm{tr}_A|\psi_0\rangle\langle\psi_0| \approx \mathrm{tr}_A|\psi_1\rangle\langle\psi_1|$,

$\exists$ a unitary on A so that $(U\otimes I)|\psi_0\rangle \approx |\psi_1\rangle$

So very good concealing $\Rightarrow$ very poor binding