How should we define post-quantum binding?

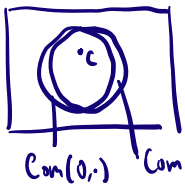
$S(m) \xrightarrow{c} R$

$w \leftarrow \{0,1\}^n$

$c = Com(m,w)$

Open: $\xrightarrow{m,w}$ Verify $Com(m,w)=c$

For today: suppose Com statistically hides m



$\Rightarrow c = Com(0,w_0) = Com(1,w_1)$

classical binding def: hard to find both. (for efficient adv)

$\tilde{S} \xrightarrow{c} R$ (Imagine $\tilde{S}$ is betting on the outcome of the election)

After election: Decide to open to m (the winner) $\xrightarrow{m,w_m}$

Obvious: if $\tilde{S}$ can do this, it can output w_0, w_1

$\Rightarrow$ break underlying assumption

(last time: find collisions in CRHF)

What if $\tilde{S}$ has a QC?

$\tilde{S} \xrightarrow{c} R$ (Communication still classical)

Decide after election which m to open $\xrightarrow{m,w_m}$

Does $\tilde{S}$ know w_0, w_1?

Detour: QC Recap

- QC can: apply efficient unitary U on $|0^n\rangle$. (recall: $U^\dagger U = I$)
- measure qubits.
- Ex: $|0^n\rangle \xrightarrow{H^{\otimes n}} \sum_{x\in\{0,1\}^n} |x\rangle|0\rangle$

$\downarrow$ any classical function f

$\sum_{x\in\{0,1\}^n} |x\rangle|f(x)\rangle$

$\downarrow$ measure

$\sum_{x\in\{0,1\}^n : f(x)=y} |x\rangle$

Hypothetical attack:

$\sum_{m,w} |m\rangle|w\rangle|Com(m,w)\rangle$

$\downarrow$ measure $=c$

$|\psi_c\rangle := \sum_{m,w: Com(m,w)=c} |m\rangle|w\rangle$ (both 0 and 1 in superposition)

$\tilde{S} \xrightarrow{c} R$

$\xrightarrow{m,w_m}$

Later, open to any bit m

$|\psi_c\rangle \xrightarrow{V_0}$ measure $= (0,w_0)$ OR $\xrightarrow{V_1}$ measure $= (1,w_1)$

① $\tilde{S}$ successfully cheats

② measurement destroys $|\psi_c\rangle$

$\Rightarrow \tilde{S}$ can't output both w_0, w_1.

Summary: Binding should imply $\tilde{S}$ can't change mind

- Classically: this means can't output w_0, w_1.
- Quantumly: new def called collapse-binding.

(Classically, def + equivalence are immediate.
Quantumly, neither def nor equivalence are obvious)

Collapse-binding [Unruh 16]

$\tilde{S} \xrightarrow{c}$ Challenger

$\sum_{m,w} \alpha_{m,w}|m\rangle|w\rangle \xrightarrow{}$

1) Verify opening:

$\sum_{m,w} \alpha_{m,w}|m\rangle|w\rangle|0\rangle$

$\downarrow$ Com

$\sum_{m,w} \alpha_{m,w}|m\rangle|w\rangle|Com(m,w)\rangle$

(if not c, abort) measure $\stackrel{?}{=} c$

② may be entangled with $\tilde{S}$'s state

2) $b \leftarrow \{0,1\}$
- If $b=0$: do nothing
- If $b=1$: measure m.

3) return $\rho_{m,w}$ (or apply Z_m)

$\rho_{m,w} \rightarrow$

b'

For all efficient $\tilde{S}$: ①

$Pr[b'=b] \leq \frac{1}{2} + negl$

Goal: understand why this says $\tilde{S}$ can't change its mind

Quantum Information

- Π is a projector if $\Pi^2 = \Pi$ and $\Pi = \Pi^\dagger$.

$U \begin{bmatrix} 1 & & \\ & 1 & \\ & & 0 \end{bmatrix} U^\dagger$

- A projective measurement $\{\Pi_i\}_i$ satisfies $\sum_i \Pi_i = I$.

$\Pi_1 = \begin{bmatrix} 1 & & \\ & 1 & \\ & & 0 \end{bmatrix}$ $\Pi_2 = \begin{bmatrix} 0 & & \\ & 0 & \\ & & 1 \end{bmatrix}$

- If I measure $|\psi\rangle$, get $\Pi_i|\psi\rangle$ w/ prob $\|\Pi_i|\psi\rangle\|^2$.

- State after measurement is a distribution over pure states. If a system is in state $|\psi_i\rangle$ w/ prob p_i, it can be described by a density matrix

$\rho = \sum_i p_i |\psi_i\rangle\langle\psi_i|$, which captures all observable properties of the system.

- Key point: many different ensembles of states can give the same ρ.

Ex: $\frac{1}{2}|0\rangle\langle 0| + \frac{1}{2}|1\rangle\langle 1| = \frac{1}{2}|+\rangle\langle +| + \frac{1}{2}|-\rangle\langle -| = \begin{pmatrix} 1/2 & \\ & 1/2 \end{pmatrix}$

ρ is a density matrix $\iff$ $\mathrm{Tr}(\rho) = 1$ and positive semidefinite $(\langle\psi|\rho|\psi\rangle \geq 0$ for all $|\psi\rangle)$

- Paulis: bit flip $X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$, phase flip $Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$ $\quad (XZ = -ZX)$

$1, -1$ eigenvectors of X are $|+\rangle = |0\rangle + |1\rangle$, $|-\rangle = |0\rangle - |1\rangle$.

$1, -1$ eigenvectors of Z are $|0\rangle$, $|1\rangle$

- Measure in standard basis $\iff$ 1) $r \leftarrow \{0,1\}$. 2) Apply Z^r.

density matrix: $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ $\xrightarrow{\text{measure}}$ $\begin{pmatrix} a & \\ & \end{pmatrix} + \begin{pmatrix} & \\ & d \end{pmatrix} = \begin{pmatrix} a & \\ & d \end{pmatrix}$

$\downarrow$ random Z^r

$\frac{1}{2}\begin{pmatrix} a & b \\ c & d \end{pmatrix} + \frac{1}{2}\begin{pmatrix} a & -b \\ -c & d \end{pmatrix} = \begin{pmatrix} a & \\ & d \end{pmatrix}$

- Overlap between two states: $|\psi_0\rangle$ and $|\psi_1\rangle$:

Prepare $\frac{1}{\sqrt{2}}(|0\rangle|\psi_0\rangle + |1\rangle|\psi_1\rangle)$, measure first qubit in $|+\rangle, |-\rangle$ basis.

Intuition: if $|\psi_0\rangle$ and $|\psi_1\rangle$ are parallel, get interference, if perpendicular, no interference.

If $|0\rangle|\psi\rangle + |1\rangle|\psi\rangle = |+\rangle|\psi\rangle$ $\Rightarrow$ always get $|+\rangle$

If $|0\rangle|\psi\rangle + |1\rangle|\psi^\perp\rangle$ $\Rightarrow$ $\frac{1}{2}$ prob of $|+\rangle$.

In general: Pr of $+$ on $|0\rangle|\widehat{\psi_0}\rangle + |1\rangle|\widehat{\psi_1}\rangle$ is $\frac{1}{2} + \mathrm{Re}(\langle\widehat{\psi_0}|\widehat{\psi_1}\rangle)$.

Goal: (1) What does "changing your mind" mean?

(2) collapse-binding $\Rightarrow$ can't change mind

(1)

$\hat{S} \xrightarrow{C} R$

Attack looks like this: $|\phi\rangle$

V_0 $\boxed{x} \to (0, w_0)$

OR

V_1 $\boxed{x} \to (1, w_1)$

Equiv: $|\psi\rangle$ $\xrightarrow{I}$ $\boxed{x} \to (0, w_0)$

- $|\psi\rangle = V_0|\phi\rangle$
- $V = V_1 V_0^\dagger$

$\xrightarrow{V}$ $\boxed{x} \to (1, w_1)$

	non attack	attack
$P_0 =$	$\frac{2}{3}$	$\frac{2}{3}$
$P_1 =$	$\frac{1}{3}$	$\frac{2}{3}$

Define projection Π_0 onto valid 0 openings w_0.

$\Pi_0 = |0\rangle\langle 0|_M \otimes \sum_{w_0 : \mathrm{Com}(0, w_0) = c} |w_0\rangle\langle w_0|$ (define Π_1 similarly)

Must guarantee:

- Adv can't open in two ways

$\|\Pi_0|\psi\rangle\|^2 + \|\Pi_1 U|\psi\rangle\|^2 = p_0 + p_1 = \mathrm{negl}$

- Adv can't change 0 opening w_0 into 1 opening w_1:

$\|\Pi_1 U \Pi_0|\psi\rangle\|^2 = \mathrm{negl}$.

Lemma:

$\|\Pi_1 U \Pi_0|\psi\rangle\|^2 = \varepsilon^2 \Rightarrow \|\Pi_0|\psi\rangle\|^2 + \|\Pi_1 U|\psi\rangle\|^2 \leq 1 + 2\varepsilon + \varepsilon^2$

(we'll prove this later).

Can't change mind $\Rightarrow$ Can't open in two ways.

suffices to show C.B. $\Rightarrow \langle\psi|\Pi_0 U^\dagger \Pi_1 U \Pi_0|\psi\rangle = \mathrm{negl}$

(2)

Why does $\langle\psi|\Pi_0 U^\dagger \Pi_1 U \Pi_0|\psi\rangle = \varepsilon$ imply distinguisher for C.B.?

($\langle\widehat{\phi_0}|$, $|\widehat{\phi_1}\rangle$)

Intuition: Want this inner product to show up distinguishing probability.

Observation: This inner product corresponds to our ability to distinguish $|0\rangle|\widehat{\phi_0}\rangle + |1\rangle U^\dagger|\widehat{\phi_1}\rangle = |\widehat{\Psi_0}\rangle$ from $|0\rangle|\widehat{\phi_0}\rangle - |1\rangle U^\dagger|\widehat{\phi_1}\rangle = |\widehat{\Psi_1}\rangle$

measure first qubit in $+,-$ basis, guess 0 if $+$, 1 if $-$.

$\Pr[\text{guess } b] - \frac{1}{2} = \frac{1}{2}[\text{measure } + \text{ on } |\widehat{\Psi_0}\rangle] - \frac{1}{2}[\text{measure } + \text{ on } |\widehat{\Psi_1}\rangle]$

$= \frac{1}{2}\left(\frac{1}{2} + \langle\widehat{\phi_0}|U^\dagger|\widehat{\phi_1}\rangle\right) - \frac{1}{2}\left(\frac{1}{2} - \langle\widehat{\phi_0}|U^\dagger|\widehat{\phi_1}\rangle\right)$

$= \langle\widehat{\phi_0}|U^\dagger|\widehat{\phi_1}\rangle = \varepsilon$.

So if $\langle\hat{\phi}_0|U^\dagger|\hat{\phi}_1\rangle = \varepsilon$, I can detect a phase flip.
Intuitively, C.B. is also about detecting a phase flip, since challenger either applies I or Z.

1) Construct $|0\rangle|\hat{\phi}_0\rangle + |1\rangle|\hat{\phi}_1\rangle$ (see below)
2) Send M, W registers of state to challenger
   - If $b=0$: get $|0\rangle|\hat{\phi}_0\rangle + |1\rangle|\hat{\phi}_1\rangle$.
   - If $b=1$: get $|0\rangle(Z_M \otimes I)|\hat{\phi}_0\rangle + |1\rangle(Z_M \otimes I)|\hat{\phi}_1\rangle$
     $= |0\rangle|\hat{\phi}_0\rangle - |1\rangle|\hat{\phi}_1\rangle$.
3) do $CT|-\rangle U^\dagger$, measure first qubit in $+/-$ basis.
   Guess $b'=0$ if $+$, $b'=1$ if $-$.

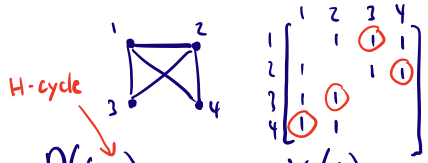
Then $\Pr[b'=b] = \frac{1}{2} + \varepsilon$.

Aside: How we prepare $|0\rangle|\hat{\phi}_0\rangle + |1\rangle|\hat{\phi}_1\rangle$
- Measure $|\psi\rangle$ w/ $\{\Pi_0, I-\Pi_0\}$.
  (If $I-\Pi_0$ outcome, give up)
- Prepare ancilla $|+\rangle$.
- Do controlled-V on $|+\rangle\Pi_0|\psi\rangle$
  to get $|0\rangle\Pi_0|\psi\rangle + |1\rangle V\Pi_0|\psi\rangle$.
- Measure w/ $\Pi' = |0\rangle\langle 0| \otimes I + |1\rangle\langle 1| \otimes \Pi_1$, get
  $|0\rangle\Pi_0|\psi\rangle + |1\rangle\Pi_1 V\Pi_0|\psi\rangle$

So far, we've seen why C.B. captures PQ binding.
Today: How do we use C.B. commitments to build PQ secure protocols?
Next time: constructing C.B. commitments

Blum's Hamiltonian Cycle Protocol

Goal: P wants to convince V that G has an H-cycle σ without revealing σ.



- $\pi \leftarrow S_n$ (permute vertices)
  Commit to each bit of $\pi(G), \pi$. $\xrightarrow{\{c_i\}_i}$
  $\xleftarrow{b}$ $b \leftarrow \{0,1\}$
- If $b=0$: open everything
  $z_0 = (\pi(G), \pi, \text{all } w_i)$ $\xrightarrow{z_b}$
- If $b=1$: only open $\pi(\sigma)$ commitments
  $z_1 = (\pi(\sigma), \text{corresponding } w_i)$

Accept if:
- $b=0$: valid perm of G and openings verify
- $b=1$: valid cycle and openings verify

Want: Completeness: Honest P always convinces V.
Soundness: If G has no H-cycle, then V accepts w/ prob $\leq \frac{1}{2} + \text{negl}$, even if $\hat{P}$ is malicious
Zero-Knowledge: $\hat{V}$ learns nothing (not today) (beyond the fact that G has an H-cycle)

Known: classical-binding commitments
⇓
Blum is sound against classical $\hat{P}$

W.T.S.: collapse-binding commitments
⇓
Blum is sound against quantum $\hat{P}$

Classical soundness of Blum

Assume $\hat{P}$ convinces V w/ prob $\frac{1}{2}+\varepsilon$.
We'll show: can extract H-cycle from $\hat{P}$.

Easy observation:
- c is "good" if $\hat{P}$ convinces V w/ prob $\geq \frac{1}{2} + \frac{\varepsilon}{2}$ conditioned on c.
- $\hat{P}$ sends good c w/ prob $\geq \frac{\varepsilon}{2}$.

$\hat{P} \xrightarrow{c} V$ ⟺

(Pf: Suppose not. Then $\hat{P}$ wins w/ prob at most $\left(1-\frac{\varepsilon}{2}\right)\left(\frac{1}{2}+\frac{\varepsilon}{2}\right) + \frac{\varepsilon}{2} = \frac{1}{2} + \varepsilon - \frac{\varepsilon}{4} - \frac{\varepsilon^2}{4} < \frac{1}{2} + \varepsilon$. Contradiction)

Rest of today: assume $\hat{P}$ wins w/ $\frac{1}{2}+\frac{\varepsilon}{2}$ prob on fixed c

Key Idea: run $\hat{P}$ on both $b=0,1$.

$\hat{P} \xrightarrow{c}$
$\xleftarrow{0}$ $\xrightarrow{z_0}$ rewind $\xleftarrow{1}$ $\xrightarrow{z_1}$

Let $p_b = \Pr_{P(b)\to z_b}[z_b \text{ valid}]$. Know: $p_0 + p_1 = 1+\varepsilon$

$\Pr[z_0, z_1 \text{ both valid}] \geq 1 - \Pr[z_0 \text{ invalid}] - \Pr[z_1 \text{ invalid}]$
$= 1 - (1-p_0) - (1-p_1) = p_0 + p_1 - 1 = \varepsilon$

Last step: if z_0, z_1 both valid, we get H-cycle.

- z_0 gives $\bar{\pi}(G), \bar{\tau}$. z_1 gives τ.
- If τ consistent w/ $\bar{\pi}(G)$, then $\bar{\pi}^{-1}(\tau)$ is Hcycle of G
- If τ inconsistent w/ $\bar{\pi}(G)$, then some commitment must be opened to both 0, 1.
  $\Rightarrow$ break classical binding.

PQ Soundness of Blum

Difficulty: if $\hat{P}$ is quantum, recording z_0 can disturb its state.

$\hat{P}$ $\xrightarrow{c}$

$\xleftarrow{0}$ $\xleftarrow{z_0}$ rewind (unclear whether $\hat{P}$ will give another valid response.)

We'll show: if commitments are C.B., possible to make rewinding work!

$\hat{P}$ has state $|\psi\rangle_{R,H}$ after sending c.

WLOG (can always redefine $|\psi\rangle, V$ to ensure this)

- To output z_0, it measures R register.
- To output z_1, it applies V, then measures R.

Let Π_b^V be projection onto accepting z_b,

$$\Pi_b^V := \sum_{z_b : V_{c,b}(z_b)=\text{acc}} |z_b\rangle\langle z_b|.$$

Assumption: $p_0 + p_1 \geq 1+\varepsilon$, i.e., $\underbrace{\left\|\Pi_0^V|\psi\rangle\right\|^2}_{p_0} + \underbrace{\left\|\Pi_1^V U|\psi\rangle\right\|^2}_{p_1} \geq 1+\varepsilon$

Ext $(U, |\psi\rangle_{RH})$:

(1) Measure $V_{c,0}(z_0) \to$ acc/rej (if rej, stop/fail)
(2) Measure $\bar{\pi}(G), \bar{\tau}$. (part of z_0)
(3) Apply U.
(4) Measure $V_{c,1}(z_1) \to$ acc/rej (if rej, stop/fail)
(5) If successful, measure τ, output $\bar{\pi}^{-1}(\tau)$.

W.t.s: Claim 1: Ext succeeds w/ prob poly(ε).
Claim 2: If Ext succeeds, it outputs H-cycle.

Pf of Claim 1

Consider Ext' that skips (2).

$|\Pr[\text{Ext' succeeds}] - \Pr[\text{Ext succeeds}]| = \text{negl}$.

If not, get efficient distinguisher against C.B.

Sub-claim: Ext' succeeds w/ prob $\Omega(\varepsilon^2)$.

Same Lemma from earlier:

If $\underbrace{\left\|\Pi_0^V|\psi\rangle\right\|^2}_{p_0=} + \underbrace{\left\|\Pi_1^V U|\psi\rangle\right\|^2}_{p_1=} \geq 1+\varepsilon$,

then $\left\|\Pi_1^V U \Pi_0^V |\psi\rangle\right\|^2 \geq \Omega(\varepsilon^2)$.

Pf of Claim 2

If Ext succeeds, why does it output an Hcycle?

- Recall: If τ and $\bar{\pi}(G)$ are consistent, then $\bar{\pi}^{-1}(\tau)$ is H-cycle of G.
- C.B. implies adv can't change mind!

$\left\|\Pi_1 U \Pi_0 |\psi\rangle\right\| = \text{negl}$, so we'll never see a 0 in $\bar{\pi}(G)$ turn into a 1 in τ

(other direction also true, but remember that V rejects if τ has any 0's)

Missing Lemma:

For projectors Π_0, Π_1, state $|\psi\rangle$, if $\left\|\Pi_1\Pi_0|\psi\rangle\right\| = \varepsilon$, then $\left\|\Pi_0|\psi\rangle\right\|^2 + \left\|\Pi_1|\psi\rangle\right\|^2 \leq 1 + 2\varepsilon + \varepsilon^2$.

(Looks different, but we can set $\Pi_0 = \Pi_0^V$ and $\Pi_1 = U^\dagger \Pi_1^V U$)

Pf: $\left\|\Pi_0|\psi\rangle\right\|^2 + \left\|\Pi_1|\psi\rangle\right\|^2$

$= \left\|\Pi_0|\psi\rangle\right\|^2 + \left\|\Pi_1\Pi_0|\psi\rangle + \Pi_1(I-\Pi_0)|\psi\rangle\right\|^2$

$\leq$ (triangle inequality) $\left\|\Pi_0|\psi\rangle\right\|^2 + \left(\left\|\Pi_1\Pi_0|\psi\rangle\right\| + \left\|\Pi_1(I-\Pi_0)|\psi\rangle\right\|\right)^2$

$= \left\|\Pi_0|\psi\rangle\right\|^2 + \varepsilon^2 + \underbrace{2\varepsilon\left\|\Pi_1(I-\Pi_0)|\psi\rangle\right\|}_{\leq 2\varepsilon} + \left\|\Pi_1(I-\Pi_0)|\psi\rangle\right\|^2$

$\leq \left\|\Pi_0|\psi\rangle\right\|^2 + \left\|(I-\Pi_0)|\psi\rangle\right\|^2 + \varepsilon^2 + 2\varepsilon = 1 + \varepsilon^2 + 2\varepsilon.$