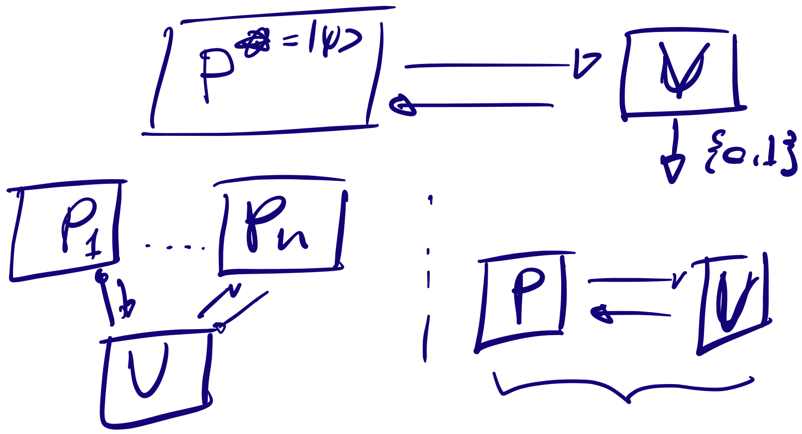
TESTING A QUBIT



- define "to have a qubit"
- TCFs
- protocol
- analysis

$\mathcal{H} \simeq \mathbb{C}^2$ $\qquad |0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \qquad |+\rangle = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 1 \end{pmatrix}$

observables: $\longrightarrow$ Heisenberg interpretation

we need two observables

mutually incompatible

BINARY OBSERVABLE

P_0 and P_1 s.t. $P_0 + P_1 = I$

$$\begin{array}{cc} P_0 & P_1 \\ \downarrow & \downarrow \\ \lambda_0 & \lambda_1 \\ = & = \\ +1 & -1 \end{array} \qquad \begin{array}{l} (-1)^0 = +1 \\ (-1)^1 = -1 \end{array}$$

$O = \lambda_0 P_0 + \lambda_1 P_1 = \sum_i \lambda_i P_i$

PROPERTIES:

① eigenvalues of O are (λ_0, λ_1)
eigenvectors of O are $|\psi_0\rangle, |\psi_1\rangle$

$$|\psi_0\rangle = P_0 |\psi_0\rangle$$
$$|\psi_1\rangle = P_1 |\psi_1\rangle$$

② O is Hermitian
$$\boxed{O^2 = I}$$

③ $\boxed{\text{Exp of } O|\psi\rangle \text{, for some } |\psi\rangle: \quad \langle\psi|O|\psi\rangle}$

$$\sum_i \lambda_i \, \mathrm{Tr}(P_i|\psi\rangle\langle\psi|) = \mathrm{Tr}\left(\sum_i \lambda_i P_i |\psi\rangle\langle\psi|\right)$$
$$= \mathrm{Tr}(O|\psi\rangle\langle\psi|)$$
$$= \langle\psi|O|\psi\rangle$$

Def. 1: A Qubit : A triple $(|\psi\rangle, X, Z)$ s.t.

① $|\psi\rangle \in S(\mathcal{H})$

② X and Z are observables on $\mathcal{H}$

③ $\underbrace{(XZ + ZX)|\psi\rangle \approx \emptyset}_{\text{anti-commute}}$ $(= \mathrm{negl}(\lambda))$

$(XZ + ZX)|\psi\rangle = 0$

$XZ|\psi\rangle + ZX|\psi\rangle = 0$

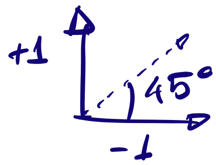
$XZ|\psi\rangle = -ZX|\psi\rangle$

let $|\psi\rangle$ be an eigenvector of X with eigenvalue ε

$X|\psi\rangle = \varepsilon|\psi\rangle$

$\langle\psi|XZ + ZX|\psi\rangle$

$$\langle\psi|(XZ+ZX)|\psi\rangle = 0$$
$$= \varepsilon\langle\psi|Z+Z|\psi\rangle$$
$$= 2\varepsilon\langle\psi|Z|\psi\rangle = 0$$



$\mathcal{H} \in \mathbb{C}^2$ $\quad |0\rangle = |\psi\rangle$

$$\underbrace{\sigma_x = \begin{pmatrix}0&1\\1&0\end{pmatrix}}_{\text{measurement in Hadamard basis}} \qquad \underbrace{\sigma_z = \begin{pmatrix}1&0\\0&-1\end{pmatrix}}_{\text{measurement in comp. basis}}$$

$+P_0 - P_1$

$\begin{pmatrix}1&0\\0&0\end{pmatrix} - \begin{pmatrix}0&0\\0&1\end{pmatrix}$

for all qubits $(|\psi\rangle, X, Z)$ on $\mathcal{H}$, there exists an isometry V:

$$V: \mathcal{H} \longrightarrow \mathbb{C}^2 \otimes \mathcal{H}'$$

① $V X|\psi\rangle = (\sigma_x \otimes I) V|\psi\rangle$

② $V Z|\psi\rangle = (\sigma_z \otimes I) V|\psi\rangle$

P

$\mathcal{H}$ $\quad V \quad$ $\mathbb{C}^2 \otimes \mathcal{H}'$

$$\begin{tikzcd}
\mathcal{H} \arrow[r] \arrow[d, "{(X,t)}"'] & \mathbb{C} \otimes \mathcal{H} \arrow[d, "{(\sigma_x \otimes I, \sigma_z \otimes I)}"] \\
\mathcal{H} \arrow[r, "V"] & \mathbb{C}^2 \otimes \mathcal{H}'
\end{tikzcd}$$

TCFs

$(td, f_0, f_1) \leftarrow Gen(1^\lambda)$

$f_0, f_1 : D \to R$

① 2-to-1: For all $y \in R$ there are EXACTLY 2 (x_0, x_1) st.

$$f_0(x_0) = f_1(x_1) = y$$

② trapdoor: $y \in R$ $\quad Invert(td, y) \to (x_0, x_1)$

③ Adaptive hardcore bit: for all QPT attacker

$$f_0, f_1 \to \boxed{A} \to (x_b, d)$$

A wins if:

$\xrightarrow{\text{comp. basis}} \circ\ x_b \in D \qquad f_b(x_b) = y$

$$\frac{1}{\sqrt{2}}|x_0\rangle + \frac{1}{\sqrt{2}}|x_1\rangle$$

$\Big\downarrow Invert(td, \cdot)$

inner prod. mod 2 $\qquad (x_0, x_1)$

Hadamard basis

- $\underbrace{d \cdot Bit(x_0) \oplus Bit(x_1)}_{\in \{0,1\}^m} = 0$
- $d \neq 0$

Prover ($|\phi\rangle = \alpha_0|0\rangle + \alpha_1|1\rangle$) | V

$(f_0, f_1, td) \leftarrow Gen(1^\lambda)$

$\sum_{x\in D}|x\rangle$

$\xleftarrow{(f_0, f_1)}$

$|\phi\rangle \sum_{x\in D}|x\rangle|0\rangle$

$= \sum_{b\in\{0,1\}} \alpha_b|b\rangle \sum_{x\in D}|x\rangle|0\rangle$

$\downarrow U_{f_0, f_1}$

$\sum_{b\in\{0,1\}} \alpha_b|b\rangle \sum_{x\in D}|x\rangle|f_b(x)\rangle \rightarrow y \in R$

$\xrightarrow{y}$

$= \sum_{b\in\{0,1\}} \alpha_b|b\rangle|x_b\rangle \cancel{|y\rangle}$

$c \leftarrow_\$ \{0,1\}$

$\xleftarrow{c=0}$

measure the 1st an 2nd register in the comp. basis

(b, x_b)

$\xrightarrow{(b, x_b)}$

ACCEPTS if $f_b(x_b) = y$

measure the 2nd register in the Hadamard basis $\xleftarrow{c = 1}$

$\xrightarrow{d \in \{0,1\}^m}$ ACCEPTS if

$d \cdot \text{Bit}(x_0) \oplus \text{Bit}(x_1) = 0$

AND $d \neq 0^m$

$(x_0, x_1) \leftarrow \text{Invert}(td, y)$