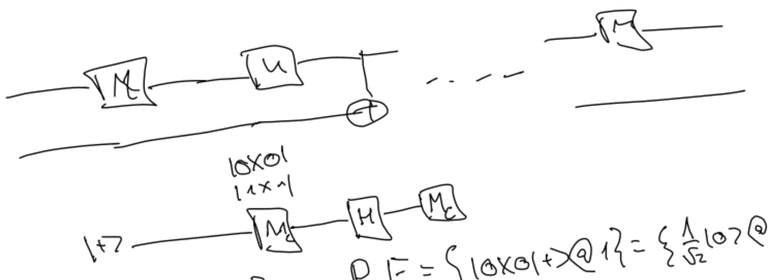

$|0\rangle\langle 0| = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$

$|0\rangle\langle 0|\,|+\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}\begin{pmatrix} 1 \\ 1 \end{pmatrix} = \frac{1}{\sqrt{2}}|0\rangle$

$P_1 E = \{ \frac{1}{\sqrt{2}}|+\rangle @ 1 \}$

$E_0 = \{ |+\rangle @ 1 \}$

$P_0 E = \{ |0\rangle\langle 0|\,|+\rangle @ 1 \} = \{ \frac{1}{\sqrt{2}}|0\rangle @ 1 \}$

$E = \{ |\psi_i\rangle @ p_i \}$

$\{Q_j\}$ projector

$E' = \left\{ \frac{Q_j|\psi_i\rangle}{\|Q_j|\psi_i\rangle\|} @ \frac{p_i \cdot \|Q_j|\psi_i\rangle\|^2}{p[\text{outcome } j]} \right\}$

$E' = \{ |0\rangle @ \frac{1}{2}, |+\rangle @ \frac{1}{2} \}$

$HE' = \{ H|0\rangle @ \frac{1}{2}, H|+\rangle @ \frac{1}{2} \} = \{ |+\rangle @ \frac{1}{2}, |-\rangle @ \frac{1}{2} \}$

$P_0 E' = \{ |0\rangle\langle 0|\,|+\rangle @ \frac{1}{2}, |0\rangle\langle 0|\,|-\rangle @ \frac{1}{2} \} = \{ \frac{1}{\sqrt{2}}|0\rangle @ \frac{1}{2}, \frac{1}{\sqrt{2}}|0\rangle @ \frac{1}{2} \}$

$P_1 E' = \{ |1\rangle\langle 1|\,|+\rangle @ \frac{1}{2}, |1\rangle\langle 1|\,|-\rangle @ \frac{1}{2} \} = \{ \frac{1}{\sqrt{2}}|1\rangle @ \frac{1}{2}, \frac{1}{\sqrt{2}}|1\rangle @ \frac{1}{2} \}$

$E'' = \{ |0\rangle @ \frac{1}{2}, |1\rangle @ \frac{1}{2} \}$

$(A \otimes B)(C \otimes D) = (AC) \otimes (BD)$
$(A \otimes B) \otimes C = A \otimes (B \otimes C)$
$(A + B) \otimes C = A \otimes C + B \otimes C$
$A \otimes (B + C) = A \otimes B + A \otimes C$

$(A \otimes B)^\dagger = A^\dagger \otimes B^\dagger$
$(A + B)^\dagger = (A^\dagger + B^\dagger)$
$(AB)^\dagger = B^\dagger A^\dagger$

Toy crypto:

Secret π

	$\pi=0$	$\pi=1$
+	$\|0\rangle$	$\|1\rangle$
X	$\|+\rangle$	$\|-\rangle$

Lecture → 1) basis = secret, value = $\pi \xleftarrow{\$} \{0,1\}$

2) basis = π, value = secret

Secret = 0, π = 1

1) $|1\rangle$ E_0 = Ensemble when secret is 0

E_1 = " " 1

2) $|+\rangle$ Lecture version:

w/ secret 0 → $E_0 = \{ |0\rangle @ \frac{1}{2}, |1\rangle @ \frac{1}{2} \}$

w/ secret 1 → $E_1 = \{ |+\rangle @ \frac{1}{2}, |-\rangle @ \frac{1}{2} \}$

Other version:

$\tilde{E}_0 = \{ |0\rangle @ \frac{1}{2}, |+\rangle @ \frac{1}{2} \}$

$\tilde{E}_1 = \{ |1\rangle @ \frac{1}{2}, |-\rangle @ \frac{1}{2} \}$

$Adv(D) = \left| P_\pi[D \text{ outputs } 1 \mid \text{secret is } 1] - P_\pi[D \text{ outputs } 1 \mid \text{secret is } 0] \right|$

D measures in diag. basis

output 1 if $|+\rangle$

$P_+ = |+\rangle\langle+| + |-\rangle\langle-|$

$P_- = |+\rangle\langle-| + |-\rangle\langle+|$

$Adv(D) = 0$

$P_\pi[D \text{ outputs } 1 \mid \text{secret is } 1] = \frac{1}{2}$

$E_1 = \{ |+\rangle @ \frac{1}{2}, |-\rangle @ \frac{1}{2} \}$

$P_+ E_1 = \{ |+\rangle @ \frac{1}{2} \}$

$P_- E_1 = \{ |-\rangle @ \frac{1}{2} \}$

$E' = \{ |+\rangle @ \frac{1}{2}, |-\rangle @ \frac{1}{2} \}$

$P_\pi[D \text{ outputs } 1 \mid \text{secret is } 0] = \frac{1}{2}$

$E_0 = \{ |0\rangle @ \frac{1}{2}, |1\rangle @ \frac{1}{2} \}$

$P_+ E_0 = \{ |+\rangle\langle+|0\rangle @ \frac{1}{2}, |+\rangle\langle+|1\rangle @ \frac{1}{2} \} =$

$= \{ \frac{1}{\sqrt{2}}|+\rangle @ \frac{1}{2}, \frac{1}{\sqrt{2}}|+\rangle @ \frac{1}{2} \}$

$P_- E_0 = \{ \frac{1}{\sqrt{2}}|-\rangle @ \frac{1}{2}, \frac{1}{\sqrt{2}}|-\rangle @ \frac{1}{2} \}$

$E' = \{ |+\rangle @ \frac{1}{2}, |-\rangle @ \frac{1}{2} \}$

$P_+ \tilde{E}_0 = \{ |+\rangle\langle+|0\rangle @ \frac{1}{2}, |+\rangle\langle+|+\rangle @ \frac{1}{2} \} = \{ \frac{1}{\sqrt{2}}|+\rangle @ \frac{1}{2}, |+\rangle @ \frac{1}{2} \}$

$P_- \tilde{E}_0 = \{ |-\rangle\langle-|0\rangle @ \frac{1}{2}, |-\rangle\langle-|+\rangle @ \frac{1}{2} \} = \{ \frac{1}{\sqrt{2}}|-\rangle @ \frac{1}{2} \}$ ($\langle -|+\rangle = 0$)

$\tilde{E}'_0 = \{ |+\rangle @ \frac{3}{4}, |-\rangle @ \frac{1}{4} \}$

$P_\pi[D \text{ outputs } 1 \mid \text{secret is } 1] = \frac{1}{4}$

$P_+ \tilde{E}_1 = \{ |+\rangle\langle+|1\rangle @ \frac{1}{2}, |+\rangle\langle+|-\rangle @ \frac{1}{2} \} = \{ \frac{1}{\sqrt{2}}|+\rangle @ \frac{1}{2} \}$

$P_- \tilde{E}_1 = \{ |-\rangle\langle-|1\rangle @ \frac{1}{2}, |-\rangle\langle-|-\rangle @ \frac{1}{2} \} = \{ \frac{1}{\sqrt{2}}|-\rangle @ \frac{1}{2}, |-\rangle @ \frac{1}{2} \}$

$\tilde{E}'_1 = \{ |+\rangle @ \frac{1}{4}, |-\rangle @ \frac{3}{4} \}$

$D \to b$

$\$ \to$

Density matrix

$E = \{ |\psi_i\rangle @ p_i \}$

$\rho_E = \sum_i p_i |\psi_i\rangle\langle\psi_i|$

$\rho_0 = \rho_1 \Rightarrow$ physically indist.

$\rho_0 = \frac{1}{2}|0\rangle\langle 0| + \frac{1}{2}|1\rangle\langle 1| = \frac{1}{2} I$

$\rho_1 = \frac{1}{2}|+\rangle\langle+| + \frac{1}{2}|-\rangle\langle-| = \frac{1}{4}\begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} + \frac{1}{4}\begin{pmatrix} 1 & -1 \\ -1 & 1 \end{pmatrix} = \begin{pmatrix} \frac{1}{2} & 0 \\ 0 & \frac{1}{2} \end{pmatrix} = \frac{1}{2} I$

$\frac{1}{\sqrt{2}}\begin{pmatrix} 1 \\ 1 \end{pmatrix}\frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \end{pmatrix} = \frac{1}{2}\begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}$ $\quad |-\rangle\langle-| = \begin{pmatrix} 1 & -1 \\ -1 & 1 \end{pmatrix}$

$\frac{1}{2}\begin{pmatrix} 1 \\ -1 \end{pmatrix}\begin{pmatrix} 1 & -1 \end{pmatrix} = \frac{1}{2}\begin{pmatrix} 1 & -1 \\ -1 & 1 \end{pmatrix}$

$E_0 = \{ |\psi_2\rangle @ 1 \}$

$\rho_0 = 1 \cdot (\varphi|\psi\rangle)(\varphi|\psi\rangle)^\dagger = \varphi|\psi\rangle \cdot (\varphi^* \langle\psi|) =$

$= \varphi\varphi^* |\psi\rangle\langle\psi| = |\varphi|^2 |\psi\rangle\langle\psi| = |\psi\rangle\langle\psi|$ ($|\varphi|^2 = 1$)

$E_1 = \{ |\psi\rangle @ 1 \}$

$\rho_1 = |\psi\rangle\langle\psi|$

Constant unitaries:

$U_f |a, b\rangle \to |a, b \oplus f(a)\rangle$

for boolean functions $A \vee B = \neg(\neg A \wedge \neg B)$

OPS = { $\neg$, $\wedge$ }

Toffoli gate

$|a, b, c\rangle \to |a, b, c \oplus (a \wedge b)\rangle$

$|000\rangle \to |000\rangle$
$|001\rangle \to |001\rangle$
$|010\rangle \to |010\rangle$
$|011\rangle \to |011\rangle$
$|100\rangle \to |100\rangle$
$|101\rangle \to |101\rangle$
$|110\rangle \to |111\rangle$
$|111\rangle \to |110\rangle$

Create Matrix based off this

$f(a,b,c) = a \wedge b \vee c$