Toy crypto example

$|0\rangle, |1\rangle$ ↓

- Alice has secret bit $b \in \{+, \times\}$ ↑ $|+\rangle, |-\rangle$
- Choose random $r \in \{0,1\}$
- Encodes r in basis b

b	r	$\|\psi\rangle$
$+$	0	$\|0\rangle$
$+$	1	$\|1\rangle$
$\times$	0	$\|+\rangle$
$\times$	1	$\|-\rangle$

- Alice sends $|\psi\rangle$ to adv.

Question: Is this protocol secure? Does b stay secret from adv?

More formally: $\forall$ adv A:

$$\Pr[A \text{ outputs } 1 : b = +] = \Pr[A \text{ outputs } 1 : b = \times]$$

Quantum state prob. distr. / ensemble

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

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

Q: Are $E_+, E_\times$ <u>physically indistinguishable</u> ?

<u>Def</u>: E, E' are physically indist.

<u>iff</u> for any Q circuit C, we have:

Prob. distrib of meas. outcomes in $C(E)$

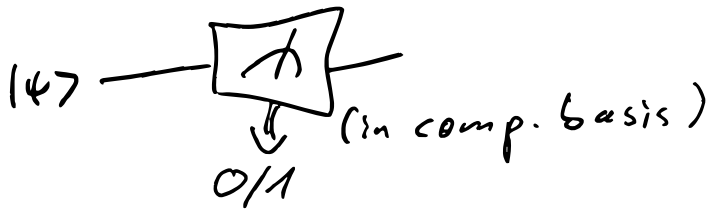
$=$ ——— " ——— in $C(E')$

Here Q circuits can contain

- Unitary ops
- Proj. meas.
- Add subsystems

Imagine trying to distinguish $E_+, E_\times$.

E.g.: Adv A:



On E_+:

$|0\rangle \rightsquigarrow 0$ (always)

$|1\rangle \rightsquigarrow 1$ (always)

$|\psi\rangle \rightsquigarrow 0 \text{ @ } \frac{1}{2},\ 1 \text{ @ } \frac{1}{2}$

On $E_\times$: $= \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle$

$|+\rangle \rightsquigarrow 0 \text{ @ } \frac{1}{2} \quad 1 \text{ @ } \frac{1}{2}$

$|-\rangle \rightsquigarrow 0 \text{ @ } \frac{1}{2} \quad 1 \text{ @ } \frac{1}{2}$

$= \frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle \quad |\psi\rangle \rightsquigarrow 0 \text{ @ } \frac{1}{2} \quad 1 \text{ @ } \frac{1}{2}$

In general: Need to show the same for <u>all</u> adv.

An approach for deciding phys. indist

1) Describe mathematically what the 3 Q circuit ops do to Q st. prob. distr.s.

2) Find a simple representation of QSPD s.t. we can compute those ops on that repr. instead.

Applying things to QSPDs:

Unitary: $E = \{ |\phi_1\rangle @ p_1, |\phi_2\rangle @ p_2, \dots \}$

$\{$ apply U

$UE = \{ U|\phi_1\rangle @ p_1, U|\phi_2\rangle @ p_2, \dots \}$

Adding subsystem:

$$E = \{ |\phi_1\rangle \otimes p_1, |\phi_2\rangle \otimes p_2, \dots \}$$

$$\Big\{ \text{appl'y } \otimes |\Gamma\rangle$$

$$E \otimes |\Gamma\rangle = \{ |\phi_1\rangle \otimes |\Gamma\rangle \otimes p_1, |\phi_2\rangle \otimes |\Gamma\rangle \otimes p_2, \dots \}$$

Measurement

$$M = \{ Q_1, \dots, Q_u \}$$

$$E = \{ |\phi_1\rangle \otimes p_1, |\phi_2\rangle \otimes p_2, \dots, |\phi_m\rangle \otimes p_m \}$$

If init. state is $|\phi_i\rangle$,

then we get:

$$\left(j, \frac{Q_j |\phi_i\rangle}{\| Q_j |\phi_i\rangle \|} \right) \text{ with prob } \| Q_j |\phi_i\rangle \|^2$$

j: outcome; $\frac{Q_j |\phi_i\rangle}{\| Q_j |\phi_i\rangle \|}$: pure

---

For $|\phi\rangle \leftarrow E$:

$$\left(j, \frac{Q_j |\phi_i\rangle}{\| Q_j |\phi_i\rangle \|} \right) \text{ with prob. } p_i \cdot \| Q_j |\phi_i\rangle \|^2$$

For $|\psi\rangle \leftarrow E$:

$$\left(j, \frac{Q_j|\phi_i\rangle}{\|Q_j|\phi_i\rangle\|} \right) \text{ with prob. } p_i \cdot \|Q_j|\phi_i\rangle\|^2$$

$$\Pr[\text{outcome } j] = \sum_i p_i \|Q_j|\phi_i\rangle\|^2$$

Given that we measured j, the post-measurement is:

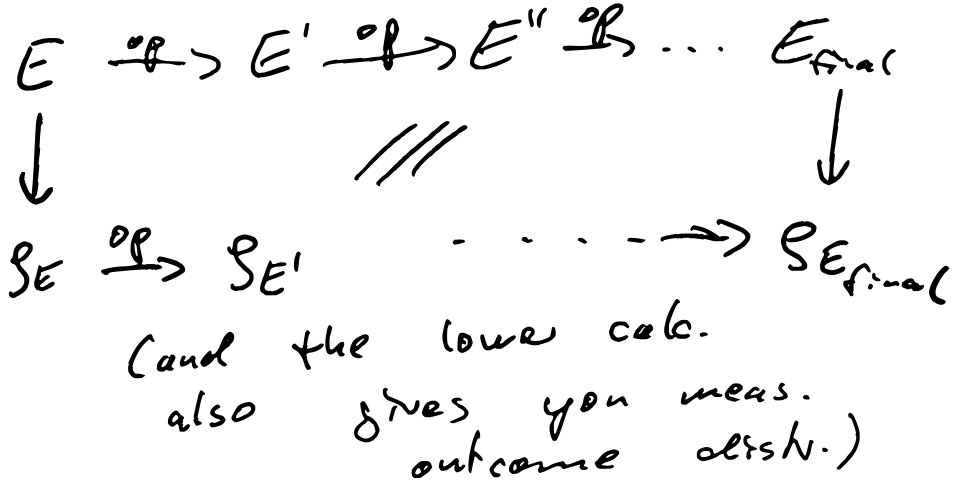
$$E_{\text{meas}\to j} = \left\{ \frac{Q_j|\phi_i\rangle}{\|Q_j|\phi_i\rangle\|} \text{ @ } \frac{p_i \|Q_j|\phi_i\rangle\|^2}{\Pr[\text{outcome } j]} \quad \text{for } i = 1 \text{ -- } n \right\}$$

Density operator:

$$E \rightsquigarrow \rho_E$$

s.t:
- From ρ_E can compute ρ_{UE}
- From ρ_E can compute $\rho_{E \otimes |\psi\rangle}$

- From ρ_E can compute:
  - $R[\text{outcome } j]$
  - $\rho_{E_{M \to j}}$



(and the lower calc. also gives you meas. outcome distn.)

Say: $\rho_E = \rho_F$ then same meas. outcome distn.

Thus: If $\rho_E = \rho_F$, then E, F phys. indist.

Def of density op for given E:

If $E = \{|\phi_1\rangle @ p_1, \ldots, |\phi_n\rangle @ p_n\}$

then $\rho_E = \sum_{i=1}^{n} p_i |\phi_i\rangle\langle\phi_i|$

$UE = \{U|\phi_1\rangle @ p_1, \ldots\}$

$$\rho_{UE} = \sum_{i=1}^{n} p_i (U|\phi_i\rangle)\cdot(U|\phi_i\rangle)^+$$

$$= \sum_i p_i U|\phi_i\rangle\langle\phi_i|U^+$$

$$= U\left(\sum_i p_i |\phi_i\rangle\langle\phi_i|\right)U^+$$

$$= U \rho_E U^+$$

$$\boxed{\rho_{UE} = U \rho_E U^+}$$

$$E \otimes |r\rangle = \{ |\phi_i\rangle \otimes |r\rangle \otimes p_i \quad (i=1\ldots) \}$$

$$\rho_{E\otimes|r\rangle} = \sum p_i \, (|\phi_i\rangle \otimes |r\rangle)(|\phi_i\rangle \otimes |r\rangle)^\dagger$$

$$= \sum p_i \, (|\phi_i\rangle \otimes |r\rangle)(\langle\phi_i| \otimes \langle r|)$$

$$= \left(\sum p_i \, |\phi_i\rangle\langle\phi_i| \right) \otimes |r\rangle\langle r|$$

$$= \rho_E \otimes |r\rangle\langle r|$$

$$\boxed{\rho_{E\otimes|r\rangle} = \rho_E \otimes |r\rangle\langle r|}$$

$$\Pr[\text{outcome } j] = \sum_i p_i \, \| Q_j |\phi_i\rangle \|^2$$

Given that we measured j, the post-measurement state is:

$$E_{\mu \to j} = \left\{ \frac{Q_j |\phi_i\rangle}{\| Q_j |\phi_i\rangle \|} \text{ @ } \frac{p_i \, \| Q_j |\phi_i\rangle \|^2}{\Pr[\text{outcome } j]} \right. \quad \left. \text{for } i = 1 \text{ — } n \right\}$$

$$\Pr[\text{outcome } j] = \sum_i p_i \, \| Q_j |\phi_i\rangle \|^2$$

$$= \sum_i p_i \, \text{tr} \left(Q_j |\phi_i\rangle \right) \left(Q_j |\phi_i\rangle \right)^\dagger$$

$$= \sum_i p_i \, \text{tr} \, Q_j |\phi_i\rangle\langle\phi_i| \, Q_j^\dagger$$

$$= \text{tr} \, Q_j \left(\sum_i p_i |\phi_i\rangle\langle\phi_i| \right) Q_j^\dagger$$

$$= \text{tr} \, Q_j \, \rho_E \, Q_j^\dagger$$

$\| |\phi\rangle \|^2 = \langle\phi|\phi\rangle = \text{tr} \, |\phi\rangle\langle\phi|$

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

$$\begin{aligned} P_r[\text{outcome } j] &= \text{tr}\, Q_j \rho_E Q_j^\dagger \\ &= \text{tr}\, Q_j \rho_E Q_j \\ &= \text{tr}\, Q_j \rho_E \end{aligned}$$

$$E_{M\to j} = \left\{ \frac{Q_j|\phi_i\rangle}{\|Q_j|\phi_i\rangle\|} \text{ @ } \frac{p_i \|Q_j|\phi_i\rangle\|^2}{P_r[\text{outcome } j]} \right\}$$

$$\rho_{E_{M\to j}} = \sum_i \frac{p_i \|Q_j|\phi_i\rangle\|^2}{P_r[\text{outcome } j]} \cdot \frac{Q_j|\phi_i\rangle}{\|Q_j|\phi_i\rangle\|} \cdot (\cdots)^\dagger$$

$$= \sum_i \frac{p_i \cancel{\|Q_j|\phi_i\rangle\|^2}\, Q_j|\phi_i\rangle\langle\phi_i| Q_j^\dagger}{P_r[\text{outcome } j]\, \cancel{\|Q_j|\phi_i\rangle\|^2}}$$

$$= \frac{Q_j \left(\sum_i p_i |\phi_i\rangle\langle\phi_i|\right) Q_j^\dagger}{P_r[\text{outcome } j]}$$

$$= \frac{Q_j \rho_E Q_j^\dagger}{P_r[\text{outcome } j]} = \frac{Q_j \rho_E Q_j^\dagger}{\text{tr}\, Q_j \rho_E Q_j^\dagger}$$

$$\rho_{E_{\mu\to j}} = \frac{Q_j \rho_E Q_j^\dagger}{\mathrm{tr}\, Q_j \rho_E Q_j^\dagger}$$

Thm: If $\rho_E = \rho_F$, then E, F are phys. indistinguishable.

(Converse also holds!)

Back to toy example

$$E_+ = \{ |0\rangle_7 \otimes \tfrac{1}{2}, |1\rangle_7 \otimes \tfrac{1}{2} \}$$

$$E_\times = \{ |+\rangle_7 \otimes \tfrac{1}{2}, |-\rangle_7 \otimes \tfrac{1}{2} \}$$

Q: Are $E_+, E_\times$ phys. indist?

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

($|0\rangle = \begin{pmatrix}1\\0\end{pmatrix}$, $|1\rangle = \begin{pmatrix}0\\1\end{pmatrix}$)

$$= \frac{1}{2} I$$

$$\rho_X = \frac{1}{2}|+X+| + \frac{1}{2}|-X-|$$

$\frac{1}{2}|+\rangle$ " $\frac{1}{2}\begin{pmatrix}1\\1\end{pmatrix}$ $\qquad$ " $\frac{1}{2}\begin{pmatrix}1\\-1\end{pmatrix}$

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

$$= \frac{1}{4}\begin{pmatrix}2&0\\0&2\end{pmatrix} = \frac{1}{2}\mathbb{I}$$

$$\Rightarrow \rho_+ = \frac{1}{2}\mathbb{I} = \rho_X$$

$\Rightarrow E_+, E_X$ phys. indist.

$\Rightarrow$ toy qubit is secure.