Toy crypto proto:

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

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

Are these phys. indist?

Density matrix / operator

$E = \{ |\phi_i\rangle \in p_i \}_i$ → ordinary proj. onto $|\phi_i\rangle$

$\downarrow$

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

$E = \{ |\phi_i\rangle \in p_i \}$ ⟶ $\rho_E = \sum_i p_i |\phi_i\rangle\langle\phi_i|$

$\downarrow U$ ⟶ $\downarrow \rho$

$UE = \{ U|\phi_i\rangle \in p_i \}$ ⟶ $\rho_{UE} = \sum_i p_i U|\phi_i\rangle\langle\phi_i|U^\dagger$

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

$= U \rho_E U^\dagger$

$\rho_{UE} = U \rho_E U^\dagger$

$\left(\frac{1}{2}\right)(+\,w) = \frac{1}{2}$

Example: $E_+ = \{ |0\rangle \in \frac{1}{2}, |1\rangle \in \frac{1}{2} \}$ ⟶ $\rho_{E_+} = \frac{1}{2}|0\rangle\langle 0| + \frac{1}{2}|1\rangle\langle 1|$

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

$\downarrow H$ ($H|0\rangle = |+\rangle$, $H|1\rangle = |-\rangle$)

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

$= HE_+$

$\rho_{E_\times} = \rho_{HE_+} = H \rho_{E_+} H^\dagger$

$= \frac{1}{2} H I H^\dagger = \frac{1}{2} I$

Adding subsystem

$E = \{ |\phi_i\rangle \in p_i \}$ ⟶ $\rho_E = \sum_i p_i |\phi_i\rangle\langle\phi_i|$

$\downarrow \otimes |r\rangle$

$E \otimes |r\rangle = \{ |\phi_i\rangle \otimes |r\rangle \in p_i \}$ ⟶ $\rho_{E\otimes r} = \sum_i p_i \left(|\phi_i\rangle \otimes |r\rangle\right)\left(\langle\phi_i| \otimes \langle r|\right)^\dagger$

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

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

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

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

Measurement

$\| |\psi\rangle \|^2 = \langle\psi|\psi\rangle = \mathrm{tr}\, |\psi\rangle\langle\psi|$

$E = \{ |\phi_i\rangle \in p_i \}$ ⟶ $\rho_E = \sum_i p_i |\phi_i\rangle\langle\phi_i|$

$\downarrow$ ⟶ $\downarrow$

$\mathbb{P}[\text{outcome } j] = \sum_{k=1}^{n} p_k \| P_j |\phi_k\rangle \|^2$

$= \sum_k p_k \langle\phi_k| P_j^\dagger P_j |\phi_k\rangle$

$= \mathrm{tr}\left(P_j \left(\sum_k p_k |\phi_k\rangle\langle\phi_k| \right) P_j^\dagger \right)$

$= \mathrm{tr}\, P_j \rho_E P_j^\dagger$

$\mathbb{P}[\text{outcome } j] = \mathrm{tr}\, P_j \rho_E P_j^\dagger$

$\mathbb{P}[\text{outcome } j] = \mathrm{tr}\, P_j \rho_E P_j^\dagger$

$= \mathrm{tr}\, P_j \rho_E$

(for measurement $P_1, \ldots$)

$E = \{ |\phi_k\rangle \in p_k \}$ ⟶ $\rho_E = \sum_k p_k |\phi_k\rangle\langle\phi_k|$

$\downarrow$ end on outcome j ⟶ $\downarrow$

$E_{\text{maj}} = \left\{ \frac{P_j|\phi_k\rangle}{\|P_j|\phi_k\rangle\|} \in \mathbb{P}[\text{outcome } j] \right\}_{k=1,\ldots,n}$ ⟶ $\rho_{E_{\text{maj}}} = \sum_k \left(\frac{p_k \|P_j|\phi_k\rangle\|^2}{\mathbb{P}[\text{outcome } j]} \right) \left(\frac{P_j|\phi_k\rangle}{\|P_j|\phi_k\rangle\|} \right) \left(\frac{P_j|\phi_k\rangle}{\|P_j|\phi_k\rangle\|} \right)^\dagger$

$= \frac{\sum_k p_k P_j |\phi_k\rangle\langle\phi_k| P_j^\dagger}{\mathrm{tr}\, P_j \rho_E P_j^\dagger}$ (with $\mathrm{tr}\, P_j \rho_E P_j^\dagger$ from above) $= \frac{P_j \left(\sum_k p_k |\phi_k\rangle\langle\phi_k|\right) P_j}{\mathrm{tr}\, P_j \rho_E P_j}$

$= \frac{P_j \rho_E P_j^\dagger}{\mathrm{tr}\, P_j \rho_E P_j^\dagger}$

$\rho_{E_{\text{maj}}} = \frac{P_j \rho_E P_j}{\mathrm{tr}\, P_j \rho_E P_j}$

(for meas. $M = \{P_0, \ldots\}$)

Conclusion

If I know ρ_E, I can compute the outcome prob. of all meas. in a seq. of ops starting from E (without knowing E)

$\Rightarrow$ If $\rho_E = \rho_{E'}$ then all outcome probs same whether we start from E or E'

$\Rightarrow E, E'$ phys. indist.

Theorem: E, E' are phys. indistinguishable iff $\rho_E = \rho_{E'}$

Back to toy crypto:

E_+, $E_\times$, $\rho_{E_+} = \frac{1}{2} I$, $\rho_{E_\times} = \frac{1}{2} I$

$\Rightarrow \rho_{E_+} = \rho_{E_\times}$ $\Rightarrow$ phys. indist

$\Rightarrow$ proto secure!

One time pad: message $m \in \{0,1\}^n$, key $k \in \{0,1\}^n$

m — $\oplus_{k=1}$ — c

Q OTP (try one) message: $|\psi\rangle \in \mathbb{C}^2$, key $k \in \{0,1\}$

$|\psi\rangle$ — X if $k=1$

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

Eg: $|0\rangle \rightsquigarrow \{ |0\rangle \in \frac{1}{2}, |1\rangle \in \frac{1}{2} \}$

$|+\rangle \rightsquigarrow \{ |+\rangle \in \frac{1}{2}, |-\rangle \in \frac{1}{2} \}$

$|1\rangle \rightsquigarrow \{ |1\rangle \in \frac{1}{2}, |0\rangle \in \frac{1}{2} \}$

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

$\rho_E = |+\rangle\langle+| + |-\rangle\langle-| = I$

$|-\rangle \rightsquigarrow \{ |-\rangle \in \frac{1}{2}, -|-\rangle \in \frac{1}{2} \}$

$\rho_E = I - |-\rangle\langle-| = |+\rangle\langle+|$

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

$X|-\rangle = -|-\rangle$

Can distinguish $\mathrm{Enc}(|+\rangle)$ and $\mathrm{Enc}(|-\rangle)$ perfectly!

Better: Q OTP message $|\psi\rangle \in \mathbb{C}^2$, key: $a \in \{0,1\}$, $b \in \{0,1\}$

$|\psi\rangle$ — X if $a=1$ — Z if $b=1$ ($(X = X^1, Z = Z^1)$)

$E = \{ |\psi\rangle \in \frac{1}{4}, X|\psi\rangle \in \frac{1}{4}, Z|\psi\rangle \in \frac{1}{4}, ZX|\psi\rangle \in \frac{1}{4} \}$

$\rho_E = \frac{1}{4}\left(|\psi\rangle\langle\psi| + X|\psi\rangle\langle\psi|X + Z|\psi\rangle\langle\psi|Z + ZX|\psi\rangle\langle\psi|XZ \right)$

$= \frac{1}{4}\left(A + ZAZ \right)$ for $A = |\psi\rangle\langle\psi| + X|\psi\rangle\langle\psi|X$

$|\psi\rangle\langle\psi| = \begin{pmatrix}\alpha\\\beta\end{pmatrix}(\bar\alpha\ \bar\beta) = \begin{pmatrix}\alpha\bar\alpha & \alpha\bar\beta\\ \beta\bar\alpha & \beta\bar\beta\end{pmatrix}$

$X|\psi\rangle\langle\psi|X = \begin{pmatrix}\beta\bar\beta & \beta\bar\alpha\\ \alpha\bar\beta & \alpha\bar\alpha\end{pmatrix}$

$A = \begin{pmatrix}\alpha\bar\alpha+\beta\bar\beta & 2\alpha\bar\beta\\ 2\bar\alpha\beta & \alpha\bar\alpha+\beta\bar\beta\end{pmatrix} = \begin{pmatrix}1 & 2\alpha\bar\beta\\ 2\bar\alpha\beta & 1\end{pmatrix}$

$ZAZ = \begin{pmatrix}1 & -2\alpha\bar\beta\\ -2\bar\alpha\beta & 1\end{pmatrix}$

$A + ZAZ = \begin{pmatrix}2&0\\0&2\end{pmatrix} = 2I$

$\rho = \frac{1}{4}(2I) = \frac{1}{2} I$ $\Rightarrow$ Q OTP is perfectly secure!

Say $|\psi\rangle = \begin{pmatrix}\alpha\\\beta\end{pmatrix}$, $|\alpha|^2 + |\beta|^2 = 1$ (for simplicity: $\alpha, \beta \in \mathbb{R}$)

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

(Caveat: Our proof did not cover the situation where the message qubit is entangled with other data)

Math fact: ρ is a density op iff

- ρ Hermitian ($\rho = \rho^\dagger$)
- $\rho \geq 0$ (all eigenvalues ≥ 0)
- $\mathrm{tr}\, \rho = 1$