# LECTURE - 21.

RECAP :

$x \leftarrow \{0,1\}, z \leftarrow \{0,1\}$ $\quad X^x Z^z \rho (X^x Z^z)^\dagger$

$x \leftarrow \{0,1\}^n, z \leftarrow \{0,1\}^n$ $\quad X^x Z^z \rho (X^x Z^z)^\dagger$.

$= X^{x[1]} \otimes X^{x[2]} \ldots$

Evaluate arbitrary quantum circuits on encrypted states

Given QOTP state

$$\sigma = X^x Z^z \rho (X^x Z^z)^\dagger ,$$ $\boxed{\text{Homomorphic enc class } (x, z)}$

If you apply a clifford $C \in \{X, Z, H, P, CNOT\}$ to the encrypted state $\sigma$,

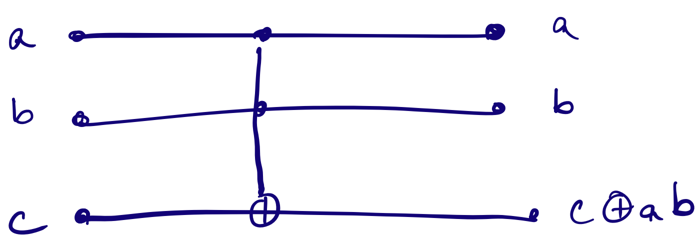
then $C \sigma C^\dagger = \underline{C X^x Z^z} \rho (X^x Z^z)^\dagger C^\dagger$

$\forall C, \forall x, z$
$\exists x', z'$ $\quad \underline{C X^x Z^z} = X^{x'} Z^{z'} C$

Substituting, $C \sigma C^\dagger = X^{x'} Z^{z'} C \rho C^\dagger (X^x Z^z)^\dagger$.

$$= QOTP_{x', z'} (C \rho C^\dagger)$$

Toffoli gate : Unitary




Start with QOTP state

$$|\psi'\rangle = X^x Z^z |\psi\rangle \quad , \text{ Enc class } (x, z)$$

$$T|\psi'\rangle = T\left(X^x Z^z |\psi\rangle\right)$$

$$|\psi_A\rangle = T X^x Z^z T^\dagger \left(T|\psi\rangle\right)$$

We would be done if this were $X^{x'} Z^{z'}$ for some $x', z'$, but that is not true.

Start with $|\psi_A\rangle = T X^x Z^z T^\dagger \left(T|\psi\rangle\right)$

convert it

$$|\psi_B\rangle = X^{x'} Z^{z'} \left(T|\psi\rangle\right).$$

Enc class $(x', z')$

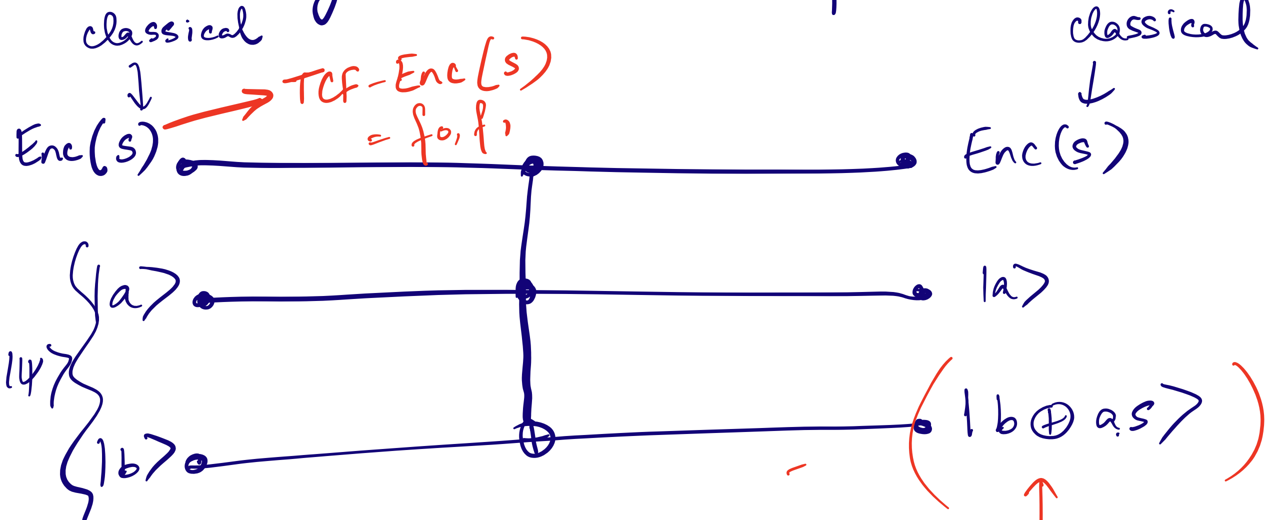
$$\left(T X^{x} Z^{z} T^{\dagger}\right)$$

$$= T\left(X^{x_1} Z^{z_1} \otimes X^{x_2} Z^{z_2} \otimes X^{x_3} Z^{z_3}\right) T^{\dagger}$$

$$= \underline{CNOT_{1,3}^{x_2}} \; \underline{CNOT_{2,3}^{x_1}} \; \tilde{Z}_{1,2}^{z_3} \underbrace{\left(X^{x_1} Z^{z_1 + x_2 z_3} \otimes X^{x_2} Z^{z_2 + x_1 z_3} \otimes X^{x_1 x_2 + x_3} Z^{z_3}\right)}_{\text{Paulis}}$$

$$\tilde{Z}_{1,2}^{z_3} = \underbrace{(\mathbb{I} \otimes H)}_{\text{clifford}} \; \underline{CNOT_{1,2}^{z_3}} \; \underbrace{(\mathbb{I} \otimes H)}_{\text{clifford}}$$

"Encrypted CNOT" operation




must be encrypted!

$X^{x} Z^{z} \, |b \oplus a s\rangle,$

$Enc(x, z)$

Given a pure quantum state $|\psi\rangle = \sum_{ab} \alpha_{ab} |ab\rangle$

$$CNOT^{s}(|\psi\rangle) \rightarrow \sum_{a,b} \alpha_{a,b} |a, b \oplus as\rangle .$$

$$CNOT^{Enc(s)}(|\psi\rangle) \rightarrow Enc\left(\sum_{a,b} \alpha_{a,b} |a, b \oplus as\rangle\right)$$

Classical Encryption

QOTP Encryption.

1) Enc(s) under the classical HE scheme

$\downarrow$ convert

special TCF - Enc(s)

2) Given TCF - Enc(s), implement Encrypted CNOT operation to obtain the QOTP - Encryption on the right.

---

TCF - Enc $(s) = (f_0, f_1)$ s.t. $\forall\, y \in Image(f_0)$,

$$x_0 = f_0^{-1}(y)$$

$$x_1 = f_1^{-1}(y)$$

$x_0 \oplus x_1$ has first bit $= s$.

Implementing Encrypted CNOT $\longrightarrow$

Goal. given $(f_0, f_1) = \text{TCF-Enc}(s)$

$$|\psi\rangle = \sum_{a,b} \alpha_{ab} |ab\rangle$$

$$\text{CNOT}^s |\psi\rangle \longrightarrow \text{Enc}\left(\sum_{ab} \alpha_{ab} |a, b \oplus as\rangle\right)$$

1) Entangle a claw with $|\psi\rangle$, i.e.

$$|\psi\rangle \hookrightarrow \sum_b \alpha_{0b} |0, b, x_0\rangle + \alpha_{1b} |1, b, x_1\rangle$$

where $(x_0, x_1)$ is a claw in $(f_0, f_1)$.

$$\sum_x |\psi\rangle |x\rangle |0\rangle = \sum_{abx} \alpha_{ab} |a\, b\, x\, 0\rangle$$

$$\Big\downarrow U_{f_0, f_1}$$

$$\sum_{abx} \alpha_{ab} |a\, b\, x\, \underline{f_a(x)}\rangle.$$

measure this register $\rightarrow$ "y"

state collapses.

$$= \sum_b \alpha_{0b} |0\, b\, x_0\rangle + \alpha_{1b} |1\, b\, x_1\rangle.$$

$$= \alpha_0 |0\ x_0[1]\ \underline{x_0[2] \ldots\ldots}\rangle + \alpha_1 |1\ x_1[1] \ldots\ldots\rangle$$

$$= \alpha_0 |0\ x_0[1]\ r_0\rangle + \alpha_1 |1\ x_1[1]\ r_1\rangle$$

$$= \alpha_0 |0\ x_0[1]\ r_0\rangle + \alpha_1 |1\ (x_0[1] \oplus s)\ r_1\rangle$$

$$= \sum_a \alpha_a |a\ x_0[1] \oplus a.s\ r_a\rangle.$$

$$\hookrightarrow \sum_{ab} \alpha_{ab} |a\ b\ x_0[1] \oplus as\ r_a\rangle$$

CNOT 3rd onto 2nd

$$= \sum_{ab} \alpha_{ab} |a\ b \oplus x_0[1] \oplus as\ x_a[1]\ r_a\rangle.$$

$$= \sum_{ab} \alpha_{ab} |a\ b \oplus as \oplus x_0[1]\ x_a\rangle.$$

$$= (I \otimes X^{x_0[1]} \otimes I)\left(\sum_{ab} \alpha_{ab} |a\ b \oplus as\ x_a\rangle\right)$$

We wanted : $X^{x'} Z^{z'} \left(\sum_{ab} \alpha_{ab} |a\ b \oplus as\rangle\right).$