LECTURE - 20.

$q = 2^{poly(m)}$.

Last time :

$$C_1 = R_1 \underset{[A, As+e]}{B} + \mu_1 G$$

$$C_2 = R_2 B + \mu_2 G$$

$$C_2 t = R_2 \cancel{Bt}^{\,e} + \mu_2 G t = (\mu_2 G t) + \text{"low norm error"}$$

Want to obtain $C^* = \mathrm{Enc}(\mu_1 \cdot \mu_2)$

C^* should decrypt to $\mu_1 \cdot \mu_2$

We want

$$\boxed{C^* t = \mu_1 \mu_2 G t + \text{"low norm error"}.}$$

$$C^* = (C_1 G^{-1}) C_2$$

$|e| \to B$.

$$C^* t = (C_1 G^{-1}) \underbrace{C_2 t}_{=(\mu_2 G t + R_2 e)}$$

$$= C_1 G^{-1} R_2 e + \mu_2 \underbrace{C_1 G^{-1} G}_{= C_1} t$$

$$= (C_1 G^{-1}) R_2 e + \mu_2 \underbrace{C_1 t}_{=(\mu_1 G t + R_1 e)}$$

$$= (C_1 G^{-1}) R e + \mu_2 \mu_1 G t + \mu_2 R_1 e$$

low norm low norm low norm

$\sim m^2 \cdot$ norm of e

"small".

$\sim m \cdot$ norm of e

$= \mu_2 \, \mu_1 \, G t \; +$ "low norm error".

(AND / XOR / NOT) are universal for classical computations.

Bootstrapping helps reduce noise in ciphertexts

What about Quantum operations?

$$c = \mathrm{QEnc}(\rho)$$

$$= X^x Z^z \rho (X^x Z^z)^\dagger \quad \mathrm{Enc}_{\text{classical}}(x, z)$$

We want to obtain $c' = \mathrm{QEnc}(X \rho X^\dagger)$

$$c = (\sigma, \underbrace{ct}_{= HE.Enc(x,z)})$$

$$\Big\downarrow ??$$

$$c' = (\sigma, \underbrace{ct'}_{= HE \cdot Enc(??)})$$

$$\text{s.t. } c' = QEnc(X \rho X^{\dagger})$$

$$\boxed{\text{I know } \sigma = X^{x} Z^{z} \rho (X^{x} Z^{z})^{\dagger} \text{ for } ct = HE.Enc(x, z).}$$

I would like ct' to encrypt (x', z')

$$\text{s.t. } \sigma = X^{x'} Z^{z'} (X \rho X^{\dagger}) (X^{x'} Z^{z'})^{\dagger}$$

$$X^{x} Z^{z} \rho (X^{x} Z^{z})^{\dagger} = X^{x'} Z^{z'} (X \rho X^{\dagger}) (X^{x'} Z^{z'})^{\dagger}$$

$$x' = x \oplus 1$$
$$z' = z.$$

To evaluate X and Z gates, just update the classical encryption.

Clifford Gates.

Include $(X, Z, H, P, CNOT)$

$\forall\, C \in \{X, Z, H, P, CNOT\}$.

$$\begin{bmatrix} 1 & 0 \\ 0 & e^{i\phi} \end{bmatrix}$$

$\forall\, (x, z)$ $\exists\, (x', z')$ such that

$\forall$ pure state $|\psi\rangle$,

$$C X^x Z^z |\psi\rangle = X^{x'} Z^{z'} C |\psi\rangle.$$

Operate on a ciphertext

$$Ct = (\sigma, ct)$$

$\sigma = X^x Z^z \rho (X^x Z^z)^\dagger$, $ct = \text{Enc}(x, z)$

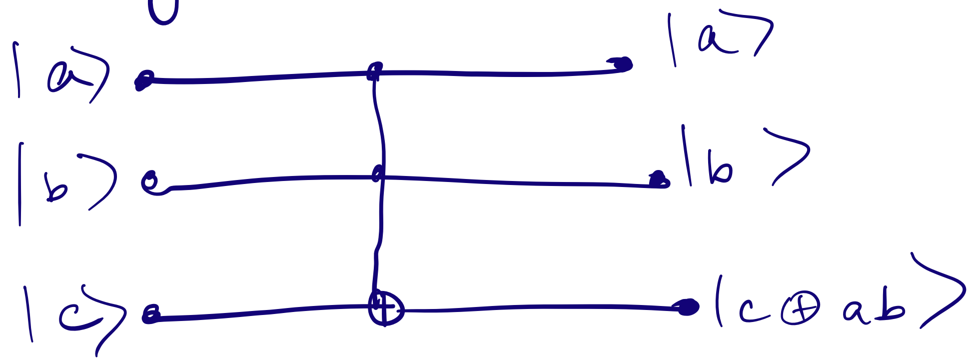
To homomorphically evaluate a Clifford gate,

replace quantum part with $\boxed{C \sigma C^\dagger}$ $\left[= C X^x Z^z \rho (X^x Z^z)^\dagger C^\dagger\right]$

By prop. of Cliffords $= X^{x'} Z^{z'} C \rho C^\dagger (X^{x'} Z^{z'})^\dagger$

replace classical part with $\text{Enc}_{\text{classical}}(x', z')$.

Toffoli gate = CCNOT



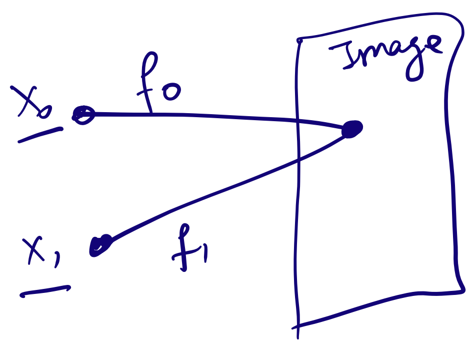
Clifford + Toffoli is universal for quantum computation

Mahadev - 2019.

TRAPDOOR CLAW-FREE FUNCTION PAIR: (TCF).

Pair of functions f_0, f_1 such that:

1) Both injective, same image



2) Hard to find a "claw"

i.e. (x_0, x_1) such that $f_0(x_0) = f_1(x_1)$

3) There is a $\boxed{\text{trapdoor}}$ td that enables efficient inversion, given any $y \in$ Image and trapdoor td, can efficiently compute (x_0, x_1) s.t. $f_0(x_0) = f_1(x_1) = y$.

How to obtain a superposition over a claw.

i.e. given (f_0, f_1), compute:

$$\frac{1}{\sqrt{2}} |0, x_0\rangle + \frac{1}{\sqrt{2}} |1, x_1\rangle$$

s.t. $f_0(x_0) = f_1(x_1)$

[By property 2 of TCF, outputting both (x_0, x_1) is hard].

1> Prepare a uniform superposition

$$|\psi\rangle = \sum_{\substack{b \in \{0,1\}, \\ x \in \{0,1\}^\lambda}} |b\rangle |x\rangle |0^\lambda\rangle .$$

2> Apply unitary

$$(b, x, y) \rightarrow (b, x, y \oplus f_b(x)).$$

to $|\psi\rangle$.

Result: $\boxed{\sum_{b \in \{0,1\}} |b\rangle |x\rangle} | f_b(x) \rangle_y$

$x \in \{0,1\}^n$

3) Measure Y register.

"y".

collapse to :

$|0, x_0\rangle + |1, x_1\rangle \otimes$ "y"

s.t. $f_0(x_0) = y$ and $f_1(x_1) = y$.

end of how to get a superposition over claws.

EXTRA PROPERTY OF TCFS :

4) There is a hidden bit s associated with (f_0, f_1) such that for <u>all claws.</u>

[i.e. all (x_0, x_1) s.t. $f_0(x_0) = f_1(x_1)$]

we have $x_0[1] \oplus x_1[1] = s$.

we have $x_0[\;] \oplus x_1[\;] = s$.

$\Longrightarrow (f_0, f_1)$ is an ENCODING/ ENCRYPTION of s.

If claws were easy to find, s would not be hidden.

Therefore,
s is hidden $\Rightarrow$ claw-freeness.

We review here the key update rules for performing stabilizer/Clifford operators on quantum data encrypted with the quantum one-time pad [Got98].

$$\mathsf{X}^{f_{a,i}}\mathsf{Z}^{f_{b,i}}|\psi\rangle \ \underset{\mathcal{X}_i}{\longrightarrow}\boxed{\nearrow}\Longrightarrow c \qquad f_{a,i} \leftarrow f_{a,i}$$

Figure 15: Protocol for measurement on the i^{th} wire: Simply perform the measurement. The resulting bit, c, can be decrypted by applying $\mathsf{X}^{f_{a,i}}$ (The key $f_{b,i}$ is no longer relevant).

$$|0\rangle \ \underset{\mathcal{X}_i}{\longrightarrow} \mathsf{X}^0\mathsf{Z}^0|0\rangle \qquad f_{a,i} \leftarrow 0, \quad f_{b,i} \leftarrow 0$$

Figure 16: Protocol for auxiliary qubit preparation on a new wire, i: Initialize a new wire labelled $\mathcal{X}_i$ and new key-polynomials $f_{i,a} = f_{b,i} = 0$.

$$\mathsf{X}^{f_{a,i}}\mathsf{Z}^{f_{b,i}}|\psi\rangle \ -\boxed{\mathsf{X}}\underset{\mathcal{X}_i}{-} \ \mathsf{X}^{f_{a,i}}\mathsf{Z}^{f_{b,i}}\mathsf{X}|\psi\rangle \qquad f_{a,i} \leftarrow f_{a,i}, \quad f_{b,i} \leftarrow f_{b,i}$$

Figure 17: Protocol for an X-gate on the i^{th} wire: Simply apply the X-gate.

$$\mathsf{X}^{f_{a,i}}\mathsf{Z}^{f_{b,i}}|\psi\rangle \ -\boxed{\mathsf{Z}}\underset{\mathcal{X}_i}{-} \ \mathsf{X}^{f_{a,i}}\mathsf{Z}^{f_{b,i}}\mathsf{Z}|\psi\rangle \qquad f_{a,i} \leftarrow f_{a,i}, \quad f_{b,i} \leftarrow f_{b,i}$$

Figure 18: Protocol for a Z-gate on the i^{th} wire: Simply apply the Z-gate.

$$\mathsf{X}^{f_{a,i}}\mathsf{Z}^{f_{b,i}}|\psi\rangle \ -\boxed{\mathsf{H}}\underset{\mathcal{X}_i}{-} \ \mathsf{X}^{f_{b,i}}\mathsf{Z}^{f_{a,i}}\mathsf{H}|\psi\rangle \qquad f_{a,i} \leftarrow f_{b,i}, \quad f_{b,i} \leftarrow f_{a,i}$$

Figure 19: Protocol for an H-gate on the i^{th} wire: Apply the gate and swap the key-polynomials.

$$\mathsf{X}^{f_{a,i}}\mathsf{Z}^{f_{b,i}}|\psi\rangle \ -\boxed{\mathsf{P}}\underset{\mathcal{X}_i}{-} \ \mathsf{X}^{f_{a,i}}\mathsf{Z}^{f_{b,i}\oplus f_{a,i}}\mathsf{P}|\psi\rangle \qquad f_{a,i} \leftarrow f_{a,i}, \quad f_{b,i} \leftarrow f_{b,i} \oplus f_{a,i}$$

Figure 20: Protocol for a P-gate on the i^{th} wire: Apply the gate and update $f_{b,i}$.

$$(\mathsf{X}^{f_{a,i}}\mathsf{Z}^{f_{b,i}} \otimes \mathsf{X}^{f_{a,j}}\mathsf{Z}^{f_{b,j}})|\psi\rangle \left\{ \begin{array}{c} \mathcal{X}_i \ -\bullet- \\ \mathcal{X}_j \ -\oplus- \end{array} \right\} (\mathsf{X}^{f_{a,i}}\mathsf{Z}^{f_{b,i}\oplus f_{b,j}} \otimes \mathsf{X}^{f_{a,i}\oplus f_{a,j}}\mathsf{Z}^{f_{b,j}})\mathsf{CNOT}(|\psi\rangle)$$

$$f_{a,i} \leftarrow f_{a,i}, \quad f_{b,i} \leftarrow f_{b,i} \oplus f_{b,j}, \quad f_{a,j} \leftarrow f_{a,i} \oplus f_{a,j}, \quad f_{b,j} \leftarrow f_{b,j}$$

Figure 21: Protocol for a CNOT-gate with control wire i and target wire j: Apply the gate and update $f_{b,i}$ and $f_{a,j}$.