Last time: \[ \text{[A, Aste]} \]

\[ C_1 = R_1 B + \mu_1 G \]

\[ C_2 = R_2 B + \mu_2 G \]

\[ C_2t = R_2 e^t + \mu_2 Gt = (\mu_2 Gt) + \text{"low norm error"} \]

Want to obtain \( C^* = \text{Enc}(\mu_1,\mu_2) \)

\( C^* \) should decrypt to \( \mu_1\mu_2 \)

We want

\[ C^* t = \mu_1\mu_2 Gt + \text{"low norm error"} \]

\[ C^* = (C_1 G^{-1}) C_2 \]

\[ |e| \rightarrow B, \]

\[ C^* t = (C_1 G^{-1}) C_2 t \]

\[ \left(\mu_2 Gt + R_2 e \right) \]

\[ = C_1 G^{-1} R_2 e + \mu_2 C_1 G^{-1} Gt \]

\[ = C_1 \]

\[ = (C_1 G^{-1}) R_2 e + \mu_2 C_1 Gt \]

\[ = \left(\mu_1 G + R_1 e \right) \]

\[ = (C_1 G^{-1}) R e + \mu_2 \mu_1 Gt + \mu_2 R_2 e \]
low norm

\sim m^2 \text{ norm } \text{ of } e

\sim \text{ small }.

= M_\sim \mu, G t + \text{ "low norm error".}

(\text{AND} / \text{XOR} / \text{NOT}) \text{ are universal for classical computations.}

\text{Bootstrapping helps reduce noise in ciphertexts}

\underline{What about Quantum operations?}

\[ C = \theta \text{Enc} (\rho) \]
\[ = X^x Z^z \rho (X^x Z^z)^+ \text{Enc}_{\text{classical}} (x, z) \]

We want to obtain \[ C' = \theta \text{Enc}(X \rho X^+) \]
\( C = (\sigma, \text{ct} = \text{HE-Enc}(x, z)) \)

\[ \downarrow \]

\( C' = (\sigma', \text{ct}' = \text{HE-Enc}(?, ?)) \)

such that \( C' = \text{QEnc}(X \rho X^*) \)

\[ \text{I know } \sigma = X^x Z^z \rho (X^x Z^z)^+ \text{ for} \]

\[ \text{ct} = \text{HE-Enc}(x, z). \]

I would like \( \text{ct}' \) to encrypt \((x', z')\)

\[ \sigma = X^{x'} Z^{z'} (X \rho X^*) (X^{x'} Z^{z'}) \]

\[ X^x Z^z \rho (X^x Z^z)^+ = X^{x'} Z^{z'} (X \rho X^*) (X^{x'} Z^{z'})^+ \]

\[ x' = x \oplus 1 \]

\[ z' = z. \]

To evaluate \( X \) and \( Z \) gates, just update the classical encryption.
Clifford Gates.

Include \((X, Z, H, P, \text{CNOT})\) \\
\(\forall C \in \{X, Z, H, P, \text{CNOT}\}\). \\
\[
\begin{bmatrix}
1 & 0 \\
0 & e^{i\phi}
\end{bmatrix}
\] \\
\(\forall (x, z) \mapsto (x', z')\) such that \(C x^z z^z |\psi\rangle = x'^z z'^z C |\psi\rangle\).

Operate on a ciphertext:

\(Ct = (\sum, ct)\) \\
\[
\begin{bmatrix}
X & Z \\
Z & X^\dagger
\end{bmatrix}
\] \(\mapsto \text{Enc} (x, z)\)

To homomorphically evaluate a Clifford gate,

replace quantum part with \(C \otimes C^\dagger\)

By prop. of Clifford:

replace classical part with \(\text{Enc}_{\text{classical}} (x', z')\).
Toffoli gate = CCNOT

\[ |a\rangle \rightarrow |a\rangle \]
\[ |b\rangle \rightarrow |b\rangle \]
\[ |c\rangle \rightarrow |c \oplus ab\rangle \]

Clifford + Toffoli is universal for quantum computation

Mahadev - 2019.
**TRAPDOOR CLAW-FREE FUNCTION PAIR:**

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 trapdoor $td$ that enables efficient inversion, given any $y \in \text{Image}$ 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.

\[ \begin{split} \text{i.e. given } (f_0, f_1), \text{ compute:} \quad & \frac{1}{\sqrt{2}} |10, x_0\rangle + \frac{1}{\sqrt{2}} |11, x_1\rangle \\ \text{s.t. } f_0(x_0) = f_1(x_1) \end{split} \]

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

\(\triangleright\) Prepare a uniform superposition

\[ |\Psi\rangle = \sum_{b \in \{0, 1\}, x \in \{0, 1\}^n} |b\rangle |x\rangle |0\rangle. \]

\(\triangleright\) Apply unitary

\[ (b, x, y) \mapsto (b, x, y \oplus f_b(x)), \]

to \(|\Psi\rangle\).

Result:

\[ \sum_{b \in \{0, 1\}} |b\rangle |x\rangle |f_b(x)\rangle. \]
3) Measure $Y$ register.

collapse to:

$$10, x_0 > + 11, x_1 > \otimes y$$

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 all claws $\{i.e. \text{ all } (x_0, x_1) \text{ s.t. } f_0(x_0) = f_1(x_1)\}$, we have $\forall \{i\} \in A \times \{i\} \Rightarrow s$. 

\[ (f_0, f_1) \text{ is an encoding/encryption of } S. \]

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].

\[ X^{f_{a,i}} Z^{f_{b,i}} |\psi\rangle \xrightarrow{X_i} c \quad f_{a,i} \leftarrow f_{a,i} \]

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

\[ |0\rangle \xrightarrow{X_i} X^0 |0\rangle \quad f_{a,i} \leftarrow 0, \quad f_{b,i} \leftarrow 0 \]

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

\[ X^{f_{a,i}} Z^{f_{b,i}} |\psi\rangle \xrightarrow{X_i} X^{f_{a,i}} Z^{f_{b,i}} X|\psi\rangle \quad f_{a,i} \leftarrow f_{a,i}, \quad f_{b,i} \leftarrow f_{b,i} \]

Figure 17: Protocol for an X-gate on the \( i \)-th wire: Simply apply the X-gate.

\[ X^{f_{a,i}} Z^{f_{b,i}} |\psi\rangle \xrightarrow{X_i} X^{f_{a,i}} Z^{f_{b,i}} Z|\psi\rangle \quad f_{a,i} \leftarrow f_{a,i}, \quad f_{b,i} \leftarrow f_{b,i} \]

Figure 18: Protocol for a Z-gate on the \( i \)-th wire: Simply apply the Z-gate.

\[ X^{f_{a,i}} Z^{f_{b,i}} |\psi\rangle \xrightarrow{H} X^{f_{a,i}} Z^{f_{b,i}} H|\psi\rangle \quad f_{a,i} \leftarrow f_{b,i}, \quad f_{b,i} \leftarrow f_{a,i} \]

Figure 19: Protocol for an H-gate on the \( i \)-th wire: Apply the gate and swap the key-polynomials.

\[ X^{f_{a,i}} Z^{f_{b,i}} |\psi\rangle \xrightarrow{P} X^{f_{a,i}} Z^{f_{b,i}} \oplus f_{a,i} |\psi\rangle \quad f_{a,i} \leftarrow f_{a,i}, \quad f_{b,i} \leftarrow f_{b,i} \oplus f_{a,i} \]

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

\[(X^{f_{a,i}} Z^{f_{b,i}} \oplus X^{f_{a,i}} Z^{f_{b,j}}) |\psi\rangle \xrightarrow{X_i} (X^{f_{a,i}} Z^{f_{b,i}} \oplus X^{f_{a,i}} Z^{f_{b,j}}) \text{CNOT}(|\psi\rangle) \]

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

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