Multi-Party Computation (MPC)
"Secure multiparty computation" (SMC)

Alice \(\xrightarrow{\text{secret}}\) 2PC \(\xrightarrow{\text{output}}\) Bob

\[ P_1 \xrightarrow{x_1} \text{MPC} \xrightarrow{x_2} P_2 \]

all get output \(o = f(x_1, x_2, x_3)\)

---

Secret Sharing

Secret Shared Backups.

long-term secret

\[ \xrightarrow{\text{backup}} \text{Cloud server} \]

written on paper

\[ \xrightarrow{\text{you could lose your backup.}} \]

\[ \xrightarrow{\text{someone else could steal your backup.}} \]

---

3-of-3 secret sharing
Using chunks...

Attacker $y$ of 2 of 3 learns part of the key (may make IND-CCA encryption insecure

Alternate:

$Y_L$, $Y_m$, $Y_H$ encrypt one of the others.

$Y' = \text{Enc}(Y_m, Y_L)$

Choose $\begin{align*}
 r_1 & \in \mathbb{Z}_q \times \mathbb{Z}_q^2 & \sqrt{\text{3rd-3}} \\
 r_2 & \in \mathbb{Z}_q \times \mathbb{Z}_q^2 & \cdot \text{can be retrieved from all 3 backup } \\
 r_3 & = r_1 \oplus r_2 \oplus y & \text{"Shares"}
\end{align*}$

- Given any two $r$ values, no information about $y$ is learned.

\[ \forall Y, \quad \exists (r_1, r_2) = U \times U \]
\[ \exists (r_2, r_3) = U \times U \]
\[ \exists (r_1, r_3) = U \times U \]

2-out-of-3: any 2 can recover $y$.

Any 1 reveals no info about $y$.

$Y' = (Y \oplus r_1) \| r_2 \| r_3$
Using polynomials

- Generalizes to any degree $K$.

Polynomials over finite fields

$\text{ex: } p(x) = 4x^2 + 3x + 2$

Degree-bound:

- How many polynomials are there over $\mathbb{Z}_7$?
  - $x^3$?
  - $x^6$?
  - $x^7$?

Avoid over counting?

- Can't be more than $|\mathbb{Z}_7| = 7$ functions

- $Q$: Do deg-bound $K$ polys form a group
\[ f(x) = a_0 + a_1 x + \ldots + a_K x^K \]
\[ = \sum_{i=0}^{K} a_i x^i \]
\[ g(x) = b_0 + b_1 x + \ldots + b_K x^K \]
\[ (f + g)(x) = (a_0 + b_0) + (a_1 + b_1) x + \ldots + (a_K + b_K) x^K \]

- Q: What about \( \text{mult} \)?
  - Both degree 2

- ex.
  \[ f(x) = x^2 \]
  \[ g(x) = 1 + 2x \]
  \[ f(x) \times g(x) = x^2 + 2x^3 \]

- Do polynomials of any degree form a group under \( \text{mult} \)?
  - Yes?

-La grange Interpolation.

Thm: given \( K+1 \) points
\[ (x_0, y_0), (x_1, y_1), \ldots, (x_K, y_K) \]
with distinct \( x_i \):
we can find a polynomial of degree \( K \) such that \( f(x_i) = y_i \) for each:

-Lemma: La grange polynomials.

Given \( K+1 \) distinct \( x \) values as above,
we can find
\[ p_i(x) \quad \text{s.t.} \quad p_i(x_s) = \begin{cases} 1 & i = s \\ 0 & i \neq s \end{cases} \]

How
\[ p_0(x) = \frac{(x-x_1)(x-x_2) \cdots (x-x_K)}{(x_0-x_1)(x_0-x_2) \cdots (x_0-x_K)} \]
\[ p_1(x) = \frac{\cdots}{\cdots} \]
\[ \vdots \]
\[ p_K(x) = \frac{\cdots}{\cdots} \]