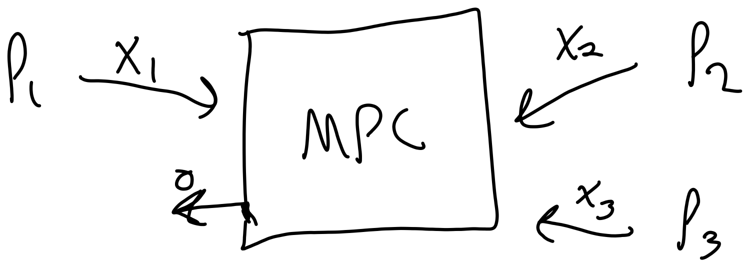
Secret Sharing I

Monday, October 18, 2021 4:00 PM

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

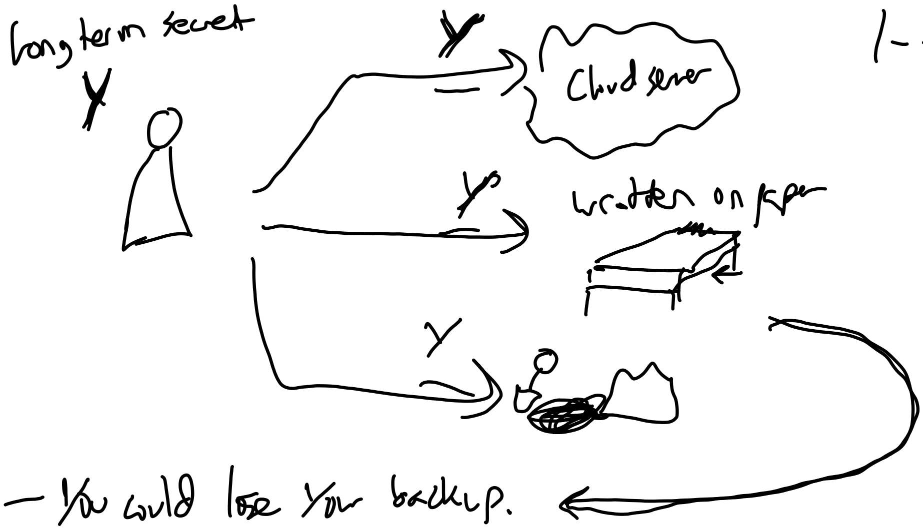


all get output $o = f(x_1, x_2, x_3)$

Secret Sharing

Secret Shared Backups.

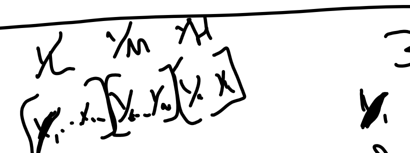
1-out-of-3

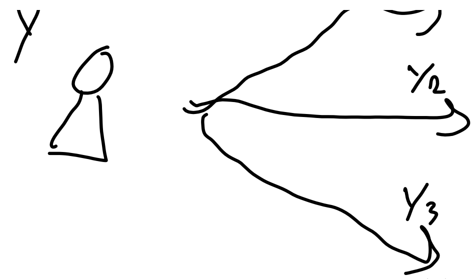


- You could lose your backup.
- Someone else could steal your backup

3-of-3 secret sharing

Chunks





* using chunks .... attacker w/ 2 of 3 learns part of the key... may make IND-CCA encryption insecure

---

Alternate? y_L y_m y_H encrypt one w/ the other.

?? $y_1' = \mathrm{Enc}(y_m, y_L)$

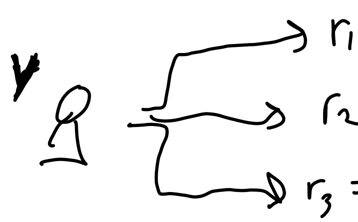
⋮

Choose $r_1 \xleftarrow{\$} \{0,1\}^\lambda$

$r_2 \xleftarrow{\$} \{0,1\}^\lambda$

✓ 3-of-3

- y can be recovered from all 3 backup "shares"
- any 2 shares reveal no info about y



$r_3 = r_1 \oplus r_2 \oplus y$

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

$\Rightarrow \forall y,\ \{r_1, r_3\} = U \times U$

$\{r_2, r_3\} = U \times U$

$\{r_1, r_3\} = U \times U$

<u>2-out-of-3</u>

- any 2 can recover y
- any 1 reveals no info about y

w/ xor? y

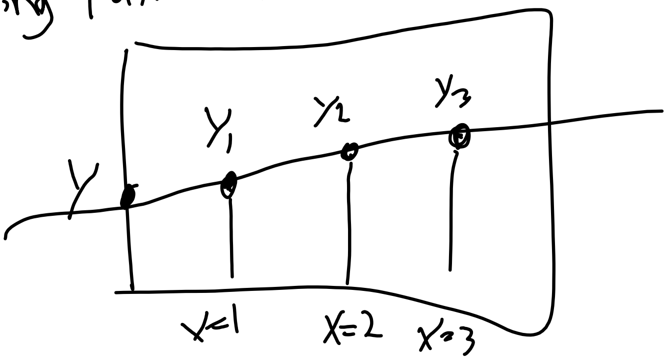
$(y \oplus r_1) \| r_2 \| r_3$

$r_1 \| (y \oplus r_2) \| r_3$

* seems to work for 2

$r_1 \| r_2 \| (y \oplus r_3)$

Using Polynomials

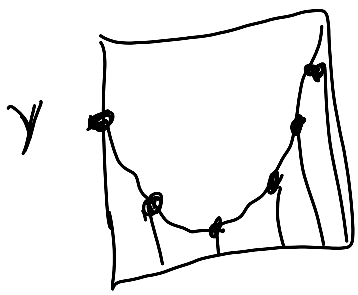


* any 2 points uniquely determine a line in 2d

* For any 1 point, every possible y is intercepted by a line through that point.

- Generalizes to any degree k.

3-of-5



- any $k+1$ points uniquely determine a degree-k or smaller polynomial

Polynomials over finite fields

ex $f(x) = 4x^2 + 3x + 2$ numbers mod p

deg 2 poly $f: \mathbb{F}_p \to \mathbb{F}_p$

finite field
- a group +
- a group × (w/o the 0 element)

Degree-bound:
≤ degree

- How many polynomials of any degree are there over $\mathbb{Z}_7$? 7^3?

~~∞~~

Avoid over counting?

- Can't be more than # of possible functions $|\mathbb{Z}_7|^{|\mathbb{Z}_7|}$

- Q: Do deg-bound k polys form a group under addition?

Coefficient representation

$$f(x) = a_0 + a_1 x + \dots + a_k x^k$$
$$= \sum_{i=0}^{k} a_i x^i \qquad g(x) = b_0 + b_1 x + \dots b_k x^k$$

$$(f+g)(x) = (a_0+b_0) + (a_1+b_1)x + \dots (a_k+b_k)x^k$$

- Q: What about mult? both deg bound 2

no. ex $f(x) = x^2$, $g(x) = 1+2x$

$$f(x) \times g(x) = x^2 + 2x^3 \leftarrow \text{not deg bound } 2$$

- Do polys of <u>any</u> degree form a group under mult?

  yes?

- Lagrange Interpolation.

  Thm: given $k+1$ points $(x_0,y_0)\ (x_1,y_1) \dots (x_k,y_k)$ w/ distinct x_i we can find a polynomial of degree-bound k s.t. $f(x_i) = y_i$ for each i

- Lemma: Lagrange polynomials

  Given $k+1$ distinct x values as above, we can find $P_i(x)$ s.t. $P_i(x_j) = \begin{cases} 1 & i=j \\ 0 & i \neq j \end{cases}$

  How

  - 1 at x_0
  - 0 at $x_1, x_2, \dots x_k$

$$P_0(x) = \frac{(x-x_1)(x-x_2)\dots(x-x_k)}{(x_0-x_1)(x_0-x_2)\dots(x_0-x_k)}$$