Problem Definition

we have m parties each has a set S_i
with $|S_i| \leq n \quad \forall i \in \{1, \dots m\}$

Threshold $t \quad 1 \leq t \leq m$

Problem

T = the set of elements that occur in at least t of the parties sets

Problem 1: find T Problem 2: find $|T|$

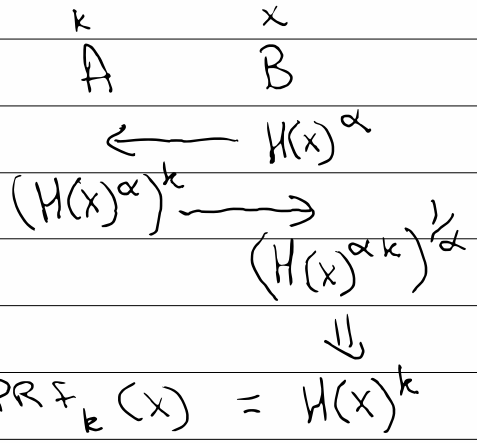
We don't want to learn:

- other elements ($\neq T$)
- how many times it occurs
- who has the elements in T
- honest but curious

Skeleton Protocol Normal Intersection

We have one k and all parties need a keyed hash of their X using k

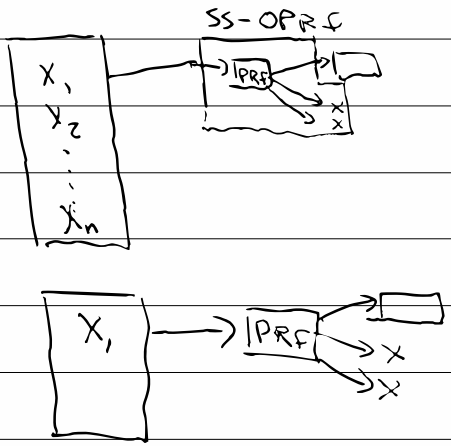
we use OPRFs:



Algo Normal Intersection

All parties calculate $OPRF_k(X_i)$
Send to trusted 3rd party who finds the intersection.
one party can reconstruct intersection as they know the mapping $x \to H(x)^k$

Skeleton t-threshold



Naive Reconstruction

$\binom{m}{t} n^t$ i.e. have to try all combinations of t shares to see what works

How to know reconstruction is valid?

S: secret → share S || SHA(S)

Note* done before starting SS-OPRF

Complexity of Reconstruction:

$k\binom{m}{t}\ell^t$ k: buckets, ℓ: bucket size

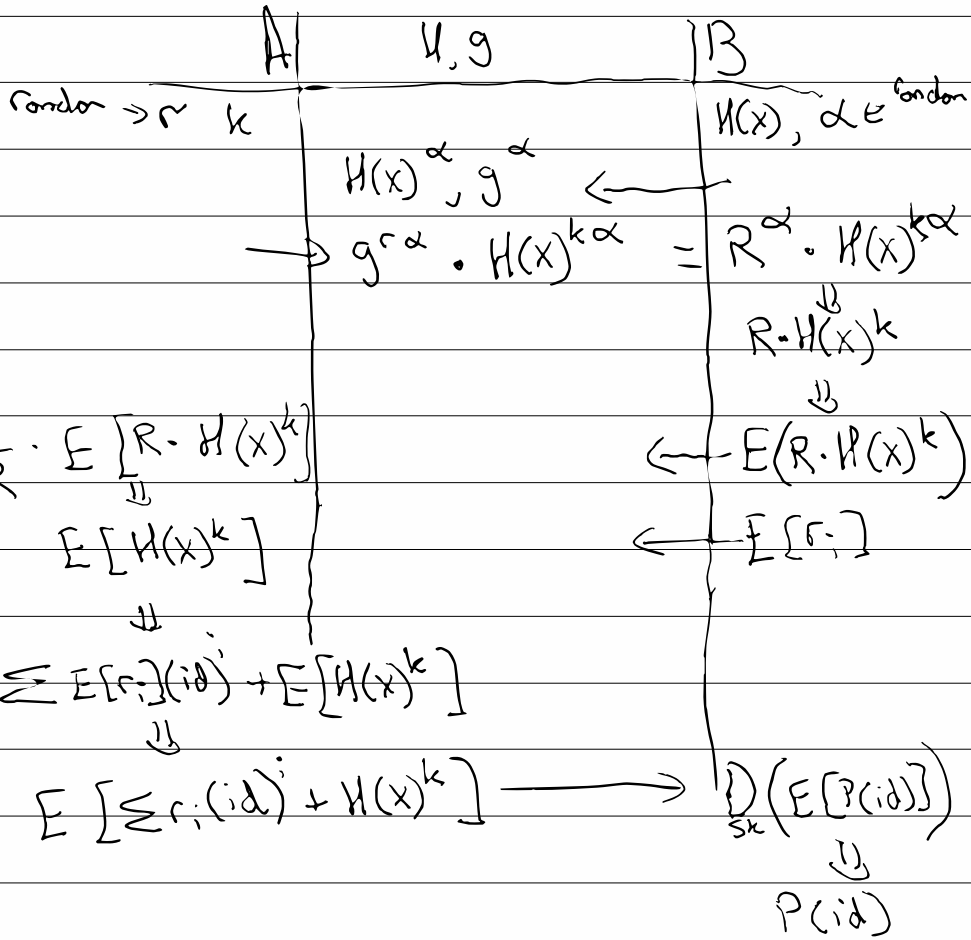
Florian's SS-OPRF

Shamir:

$$P(x) = \sum_{i=1}^{t} r_i x^i + S$$

Secret $H(k, x) = H(x)^k$

$$P(x_j) = \sum_{i=1}^{t-1} r_i x_j^i + H(x)^k$$



reconstruction (Shamir)

$$P(x) = \sum_{i=0}^{t} P(x_i) \prod_{j \neq i} \frac{(x - x_j)}{(x_i - x_j)}$$

$$P(0) = \sum_{i=0}^{t} P(x_i) \prod_{j \neq i} \frac{-x_j}{(x_i - x_j)} = S$$

Rasoul's SS-OPRF

Secret Sharing in the exponent:

Recall Shamir: $P(x) = \sum_{i=1}^{t} r_i x^i + S$

$$f(x) = g^{P(x)}$$

So, reconstruction

$$g^{\sum P(x_i) \prod_{j \neq i} \frac{(x - x_j)}{(x_i - x_j)}}$$

$$= \prod f(x_i)^{\prod_{j \neq i} \frac{(x - x_j)}{(x_i - x_j)}} = f(x)$$

$$f(0) = \prod f(x_i)^{\prod \frac{-x_j}{x_i - x_j}} = g^S$$

$$f(x_i) = g^{P(x_i)} = g^{\sum r_i x^i + s} = g^{\sum r_i x^i} \cdot H(x)^k$$