Problem Def

m parties

party i has set S_i

$|S_i| \leq n$

t: threshold $1 \leq t \leq m$

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

problem 1: T

problem 2: $|T|$

Not learn:

- other elements $(\overline{T})$
- who has the elements in T
- how many times it occurs

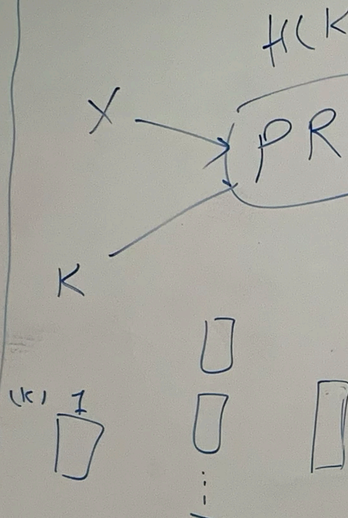
not learn

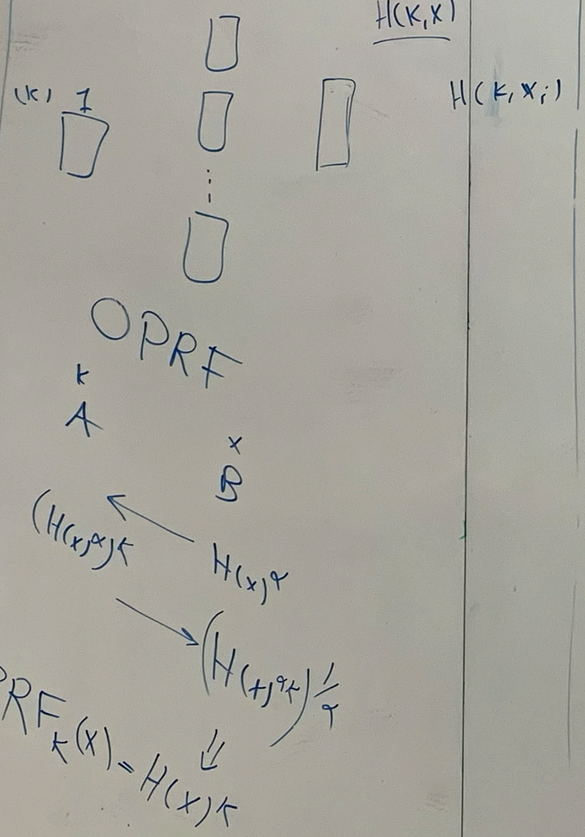
- honest b.c.

$H(x)^\alpha = (H(x)^2)^{\alpha/2}$

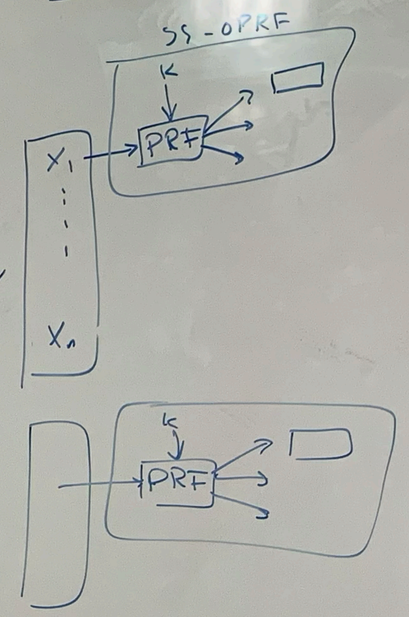
$H(x)^\alpha = (\text{---}) = A\,B$

Skeleton Protocol intersection





skeleton t-threshold



Naive reconstruct

$\binom{m}{t} n^t$

How to know reconstruction is valid?

S: secret → share $S \| S \oplus H(S)$

Shamir

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

$P(X_i)$ share

FSS

secret $H(K,X) = H(X)^K$

$$P(X_j) = \sum_{i=1}^{t-1} r_i X_j^i + H(X)^K$$

$X_j = j$

(K') A	H, g	B (X)
	$\overset{K}{\leftarrow}$	
random $\leftarrow r$	$H(X)^\alpha, g^\alpha$	$H(X)^\alpha$ α random
	$\rightarrow g^{\alpha r} \cdot H(X)^{\alpha K}$	$R \cdot (H(X)^K)$

Context 1 (Florians) { Prime P; generator g; $H(\cdot)$, $H_B(\cdot)$; $Enc(\cdot)$, prime P, q

Context { P, q ($P = 2q+1$); g (if necessary); $H(\cdot)$, $H_B(\cdot)$ (hard code)

C, C++

Integer Library : NTL? (Rasoul)

Context 1/2 + $r_1, \ldots, r_{t-1}, K_1, K_2$ → ShareGen → $(id, bin, SS(H(x)^{K_1}; id), SS(H(x)^{K_1 K_2}; id))$

$q = (id, bin, SS, \ldots, SS_M)$

Context 2 { prime $P = 2q+1$; prime q; $H(\cdot)$, $H_B(\cdot)$

Context 1/2 + $q_1, q_2, \ldots, q_t$ → Rcon → T/F

TODO: Find benchmarkable parameters

$\frac{n}{\log n} \binom{m}{t}$

(format?)

X

$H(x)$

$r_1, \dots, r_t$

$H(x)^{\alpha}, g^{\alpha}$

g^{h_x} $\quad g^{\alpha \sum r_i (id)^i}$ $\quad \leftarrow$

$g \cdot H(x)^{k\alpha} \longrightarrow g^{r_i}$

$P < 2(q) + 1$ $\quad H(x)^{r_i}$ $\quad g^{h_x r_i}$ $\quad H(x)$ $\quad \alpha \sum r_i (id_i \dots$

$H(x)^\alpha, g^\alpha$

$\longrightarrow g^{kr} \cdot H(x)^{\alpha k} \mod p'$

$\longleftarrow E(g^r \cdot H(x)^\alpha) \mod pq$ ($g^r \mod p'$)

$R = [0, p'-1 \cdot 2^{80}] \cdot p'$

$E(R + H(x)^\alpha)$

$\mod p' \longrightarrow H(x)^q$

$p = 2q+1$

$pq > (p')^2 \cdot 2^{80}$ g_n

$g \quad G_p$

$G_q \quad g_n = g^2$

G_q

$\mod 7 = 2 \cdot 3 + 1$

$3 | 2, 6, 4, 5, 1$

$2, 4, 1$

$p | \phi(s)$

$s = p^n q^m \quad \phi(s) = (p-1)p^{n-1} \cdot (q-1)q^{m-1}$

$x^{\phi(s)} = 1 \mod s$

$a^r == a^{r \bmod \phi(s)} \mod s$

$(a^p)^r == (a^b)^{r \bmod \frac{\phi(s)}{p}}$

$\sum r_i x_k^i + S = Y_k$

(x_i, y_i) : t shares

$$= \sum_{i=\emptyset}^{t} y_i \prod_{j \neq i} \frac{x - x_j}{x_i - x_j}$$

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

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

$= g^{\sum r_i x_k^i + S}$

share : $f(x_k) = g$ $= g^{\sum r_i x_i} \cdot g^S$

$\emptyset) = g^{\sum y_i \prod \frac{-x_j}{x_i - x_j}}$

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

$= g^S$

$= H(x)^{k_1} = g^{S'}$

$\phi(p)$

prime $p \overset{?}{=} 2q+1$, generator g

$p-1 = 2q$

Keyholder k_1, k_2

randoms $\overset{p^*}{\rightarrow} r_1, \ldots, r_{t-1}$

Keyholder (K)	Element holder (X)

random $\rightarrow \alpha$

$g^{\alpha \sum (id)^i r_i} \cdot H(x)^{\alpha k_1}$ $\leftarrow$ $H(x)^\alpha, g^\alpha, id$

$\rightarrow g^{\frac{\sum (id)^i r_i \; k_1}{H(x)}}$

$\{ H(x)^{r_i (id)^i} + H(x)^{k_1}$

$\sum$

why
the sun
sunglass

2

$a \; a^* \overset{p}{=} 2$

$H_B(\cdot)$

* bins are padded to size max

prime p, generator g

$H(\cdot)$, $H_B(\cdot)$

Keyholder: K_1 K_2

randoms $\xrightarrow{P} r_1, r_2, \ldots, r_{t-1}$

randoms $\xrightarrow{P} s_1, s_2, \ldots, s_{k-1}$

Keyholder (K_1)	Element holder (X)
Round 1	random $\xrightarrow{P} \alpha$
random $\xrightarrow{P} r$	$H(x)^\alpha, g^\alpha, id$
Round 2 $g^{r\alpha} \cdot H(x)^{k_1 \alpha}$	$R^\alpha \cdot H(x)^{\alpha k_1}$
$g^{r\alpha} \cdot H(x)^{r_i \alpha}$ for each r_i	$R^\alpha \cdot H(x)^{\alpha r_i}$ for each r_i
	* choose Enc scheme
	$E[R \cdot H(x)^{k_1}]$
mult by $1/R$	$E[R \cdot H(x)^{r_i}]$ for each r_i
$Enc[H(x)^{k_1}]$	
$E[H(x)^{r_i}]$	
$\sum (id)^i \cdot E[H(x)^{r_i}]$	$H_B(x) \bmod \#bins$, id
$+ E[H(x)^{k_1}]$	$SS(H(x)^{k_1}, id)$
$= E[SS(H(x)^{k_1}, id)]$	$SS(H(x)^{k_1, k_2}, id)$

MAC

Normal SS

$f(X_K) = \sum r_i X_k^i + S = Y_K$

(x_i, y_i) : t shares

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

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

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

share: $f(x_k) = g^{\sum r_i x_k^i + S} = g^{\sum r_i x_i} \cdot g^S$

$f(\emptyset) = g^{\sum y_i \prod \frac{-x_j}{x_i - x_j}}$

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

$= g^S$

$= H(x)^{k_1} = g^{S'}$

p

$\phi(p)$

prime $p \stackrel{?}{=} 2q+1$, generator g

Keyholder k_1, k_2

randoms $\xrightarrow{P^*} r_1, \ldots, r_{t-1}$

Keyholder (K)	Element holder (X)
	random $\rightarrow \alpha$
$g^{\sum (id)^i r_i} \cdot H(x)^{\alpha k_1}$	$\leftarrow H(x)^\alpha, g^\alpha, id$
$\rightarrow g^{\sum (id)^i r_i} H(x)^{k_1}$	$\sum H(x)^{r_i \cdot (id)^i} + H($

PRF-GEN

r

$k_1 = SS(r, id=1)$

k_2 $SS(r, id=2)$

$H(1)^{SS(r)_{id}}$

$SS(H(1))_{id}$

id=1

id=2

1^{k_1} 2^{k_1} 3^{k_1}

2^{k_2} 3^{k_2} 4^{k_2}

2^r 3^r

recon:

$\binom{m}{t}$ $\binom{t}{0,n}$

r_1 r_2 r_3

$H(1)^{r_1}$ id^2

$H(1)^{k_1}$ id

$H(1)^r$

$H(1)$

$H(2)$

$H(3)$

$S = H(1)^r$

$H(1)^{k_1 r} \leftarrow H(1)^{\alpha}$

r_1 r_2 r_3

A K B Y

r

$H(m)^{\alpha}, g^{\alpha}$

$H(m)^{r\alpha} \cdot H(m)^{k\alpha} \rightarrow R \cdot H(m)^k$

$H(m)$ α

$P(x) = \sum r_i x^i$ $SS(R_m^{-1})$

$\rightarrow SS(H(m)^k)$

$P(1) = \sum_i id^i + R_m^{-1}$

$P_1(x) = c + R_1^{-1} m$

$P_2(r) = c + R_2^{-1} m$

$R_{1,m}^{-1}$ $R_{2,m}^{-1}$

$m \cdot |R|$

$|c| = |R|$

$c, H(m)^m$

SS-OPRF

1 K

2 m $H(m)^k$

$H(m)^\alpha$

g^α

$h(m) = (g^\alpha)^{\sum r_i x^i} H(m)^{\alpha k} \longrightarrow \left(g^{\alpha \sum r_i x_i^i} H(m)^{\alpha k}\right)^{1/\alpha}$

$g^{\sum r_i x_i^i}$

$\cdot H(m)^k = g^{\sum r_i x_i^i + s'}$

$H(m)^k = g^{s'}$

$h(X) = g^{P(X)}$

$(x_i, h(x_i))$

$h(x_i) = g^{P(x_i)}$

P. 129

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

$= \prod h(x_i)^{\prod \frac{X-y_j}{x_i-x_j}}$

$h(x_i)^{z^\alpha}$

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

$(x_i, P(x_i))$

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

ORRF

ORRF-comm

Recv comm

Recv

m: number of part

$D_1 < n$

$P1: (x-a)^t \mid P(x) \rightarrow x-a \mid P^{(t-1)}(x)$

$R_{(a,b)}(x) = P_a(x) \cdots P_{b-1}(x)$

$R_{[1,m+1)} = R_{[1,m)} \cdot P_m(x)$

$\rightarrow O(t^m)$

$O(t.m)$

$Q(x) = P_1(x) . P_2(x) \cdots P_m(x)$

$Q(x) = q_p x^p + \cdots + q_1 x + q_0 \rightarrow m^2 n$

$Q'(x) = q_1 . p . x^{p-1} + \cdots$

$Q^{(t-1)}(x) =$

$q_{1,1-1} \rightarrow x(x-1)(x+1) = x^3 - x \rightarrow 3x^2 - 1 \rightarrow 6x$

$O(mn)$

x^2+x+1

$2x^4 + 3x^3 + 4x^2 + 2x + 1$

$R(x) = Q(x) + Q'(x) + \cdots + Q^{(t-1)}(x)$