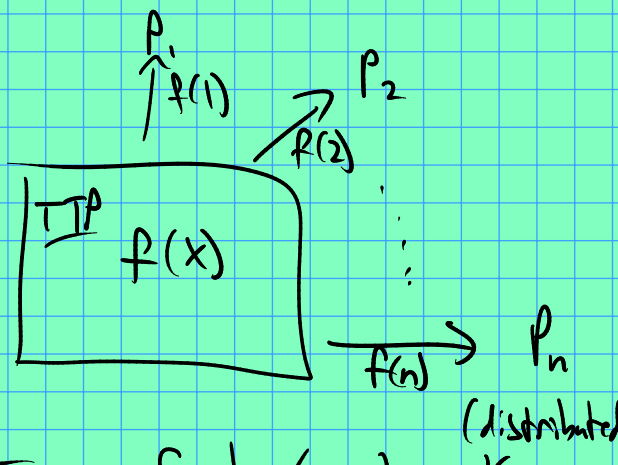
Re-sharing secrets:

$$f(x) = s + c_1 x + c_2 x^2 + \cdots c_t x^t \qquad c_i \in_R \mathbb{F}_p \qquad s \in \mathbb{F}_p$$



(distributed!)

To refresh/reshare one idea is for each P_i to generate a random poly f_i of degree t w/ $f_i(0) = 0$. (constant term is 0).

Now P_i sends to P_j $\underline{f_i(j)}$ $\forall\, i, j \in [n]$.

(Each player distributes shares of 0 to each other...)

Now shares: $[\text{old share}]_i + \sum_{j=1}^{n} f_j(i)$ (P_i's computation)

$$f(i) + f_1(i) + \cdots + f_n(i)$$

$$= \underline{\left(f + \sum_{j=1}^{n} f_j\right)(i)}$$

call this polynomial f'. $f'(0) = s$.

And each P_i has $f'(i)$!

Moreover, if at least one player chose f_j randomly, resulting f' is random!

(Note: similar technique used in distributed key gen say for ElGamal.)

#7: Random-self-reducible: ability to solve random instances $\Rightarrow$ ability to solve any instance.

Either almost all instances are easy, or almost all are hard.

DLP: Say $\exists\ O$ s.t. $\Pr_{a \in_R \mathbb{Z}_q}[O(g^a) = a] \geq 1/\text{poly}$.

Say we are given $y = g^x$.

Solution using O: produce $y' = y g^r$, $r \in_R \mathbb{Z}_q$.

y' is uniform in $\langle g \rangle$! So O "works" on it.

if O produces a solution to y', we will know $x+r$ and hence x!

until (O is right on $y' = y g^r$) choose new $r \in_R \mathbb{Z}_q$ } poly(l)

$x' = O(y')$

output $x' - r$ $(= x)$ ✓

Our odds of success are $1 - \text{negl}(l)$ independent of x.

Similar thing works for RSA...