Algo Notes

January 31, 2020

m = # of parties

n = max set size per party

t = threshold (both thresholds, intersection and the secret sharing threshold)

Each bin is padded to max.

Assumptions:

- Keyholder is semi-honest
- Keyholder is not a party
- Keyholder sees at most $t-1$ shares (ever)

Scheme F

prime p, generator g

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

Keyholder: K_1, K_2

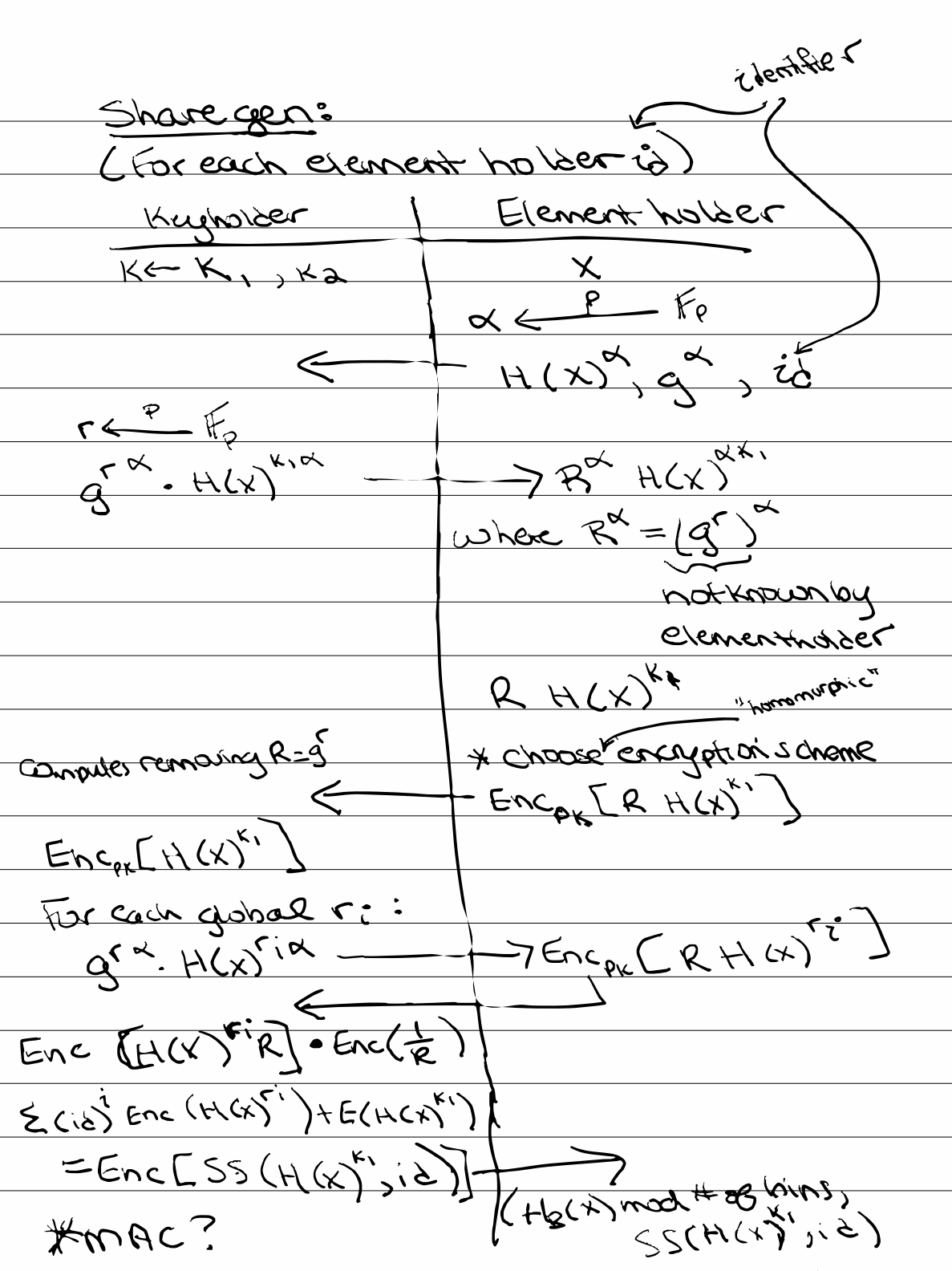
$r_1 \cdots r_{b-1} \leftarrow \mathbb{F}_p$

} set up / global randoms

Share gen on next page.

"Homomorphic" Enc Scheme

- PK, SK, $Enc(\cdot)$


identifier
Share gen:
(For each element holder id)
Keyholder
Element holder
K ← K1, ..., Ka
x
α ← p — Fp
H(x)^α, g^α, id
r ← p — Fp
g^rα · H(x)^K1,α
R^α H(x)^αK1
where R^α = (g^r)^α
not known by element holder
R H(x)^K1
"homomorphic"
* choose encryption scheme
Computes removing R=g^r
Enc_pk[R H(x)^K1]
Enc_pk[H(x)^K1]
For each global ri:
g^rα · H(x)^ri α
Enc_pk[R H(x)^ri]
Enc [H(x)^ri R] • Enc(1/R)
Σ(id)^i Enc(H(x)^ri) + E(H(x)^K1)
= Enc[SS(H(x)^K1, id)]
(hb(x) mod # of bins, SS(H(x)^K1, id))
*MAC?

Recon:

Each participant sends their shares to the reconstructor $\mathcal{R}$ who is a participant

For each bin

For each $\binom{m}{t}$ subset of the participants

- use Lagrange interpolation

↳ magically validate it for our t requirements.