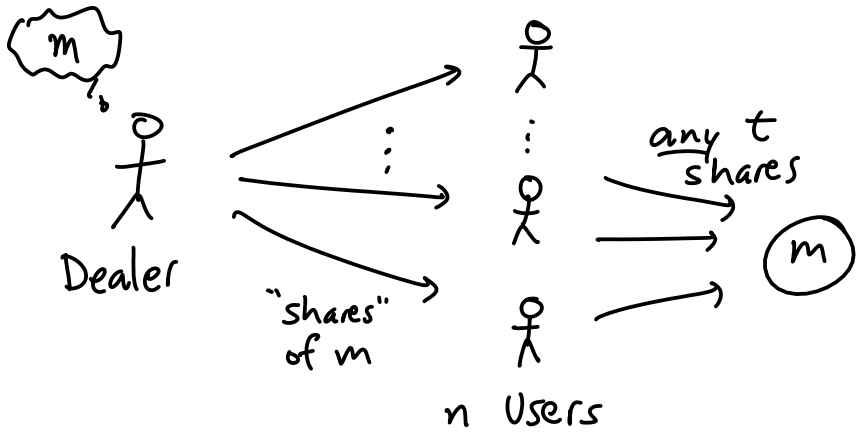
Secret-Sharing Schemes

- HW1 due Friday !
- office hours M, W after class



t = threshold

Syntax: A t-out-of-n threshold secret sharing scheme (SSS) consists of:

- $\text{Share}(m) \longrightarrow (s_1, \ldots, s_n)$ // randomized
  - m: secret; $(s_1, \ldots, s_n)$: shares
  - user #i gets s_i
- $\text{Reconstruct}\left((s_i)_{i \in \mathcal{U}}\right) \longrightarrow m$ // where $\mathcal{U} \subseteq \{1, \ldots, n\}$, $|\mathcal{U}| \geq t$
  - $(s_i)_{i \in \mathcal{U}}$: set of shares belonging to users whose id $\in \mathcal{U}$.

Correctness:

If $|\mathcal{U}| \geq t$ then for all m:

if $(s_1 \cdots s_n) \leftarrow \text{Share}(m)$

then $\text{Reconstruct}\left((s_i)_{i \in \mathcal{U}}\right) = m$

Terminology:

$|\mathcal{U}| \geq t$: $\mathcal{U}$ is authorized

$|\mathcal{U}| < t$: unauthorized

Security: "unauthorized set of shares leaks no info about m"

Idea: Define 2 libraries, same interface

interface should let caller see un authorized set of shares

only diff between libs is choice of m

which set of shares?
which m to secret-share?
⇒ let Adv (calling prog) choose!

Def: SSS is secure if

$\mathcal{L}_{tsss-L}$:

```
Query(m_L, m_R, U):
    if |U| ≥ t : abort
    s⃗ ← Share(m_L)
    return (s_i)_{i∈U}
```

$\equiv$

$\mathcal{L}_{tsss-R}$:

```
Query(m_L, m_R, U):
    if |U| ≥ t : abort
    s⃗ ← Share(m_R)
    return (s_i)_{i∈U}
```

only allow Adv to see an unauthorized set of shares

Note: example: 5-out-of-8 SSS ($t=5$)

Adv can ask for U with $|U| \leq 4$

but Adv can ask for users $1, \ldots, 4$ in one call

$5, \ldots, 8$ in another

⇒ 2 calls to Share (rand. alg.) give independent sets of shares, no reason for the 2 sets of shares to be correlated

Simple Construction: (2-out-of-2 SSS)

$\{1\}$ unauthorized $\Rightarrow$ s_1 alone : no info m

$\{2\}$ unauth. $\Rightarrow$ s_2 alone: no info

$\{1,2\}$ auth. $\rightarrow$ s_1, s_2 together: reveal m

Idea: In one-time pad:

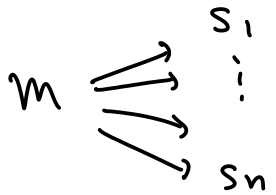
key by itself: indep. of ptxt

ctxt by itself: indep. of ptxt

key, ctxt together: Dec to learn ptxt

[see supplementary slides]

Q: What about 3-out-of-3 ? n-out-of-n ?



where $s_1 \oplus \cdots \oplus s_n = m$

i.e.,

$s_1 \leftarrow \{0,1\}^\ell$

$s_2 \leftarrow \{0,1\}^\ell$

$\vdots$

$s_{n-1} \leftarrow \{0,1\}^\ell$

$s_n = m \oplus s_1 \oplus \cdots \oplus s_{n-1}$