- Course webpage:
  - http://www.cs.umd.edu/~jkatz/gradcrypto2/S21
- If taking the course for credit:
  - Scribe lecture notes (in pairs, ~2x per semester)
  - midterm + final
- No prior background assumed, but course will move quickly
- Syllabus (w/ optional readings) updated throughout semester
  - tentative plan:
    - ~50% secure computation
    - ~15% each on diff. privacy, "blockchain," and SNARKs/ZK proofs
    - 5% other topics
  - suggestions welcome!
- Interaction welcome!

  Please keep video on

Indistinguishability of distribution ensembles

- negligible functions: function $f: \mathbb{N} \to [0,1]$ is negligible if for all c there exists N s.t. for $k \geq n$, $f(k) \leq 1/k^c$.
- distribution ensembles $\{X(k,a)\}_{k \in \mathbb{N}, a \in \{0,1\}^*}$, $\{Y(k,a)\}_{k,a}$

Statistical/perfect indistinguishability

perfect: $\forall k, a$, $X(k,a) = Y(k,a)$

statistical X, Y are ε-close if $\forall k, a$, $SD(X(k,a), Y(k,a)) \leq \varepsilon(k)$

$$SD(X,Y) = \frac{1}{2} \sum_a \left| Pr[X=a] - Pr[Y=a] \right|$$

Computational indistinguishability

... if for all prob. poly-time distinguishers D, there is a negl. function ε s.t. for all a, z

$$\left| Pr[D(k,a,z,X(k,a)) = 1] - Pr[D(k,a,z,Y(k,a)) = 1] \right| \leq \varepsilon(k)$$

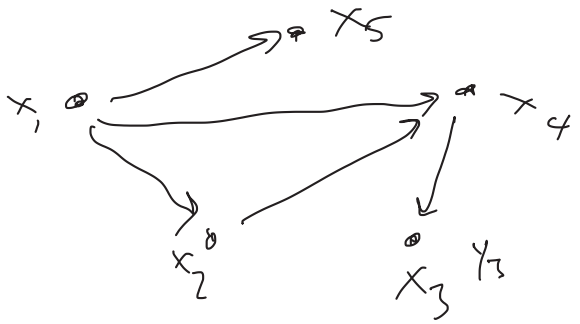
auxiliary input

$$Pr[x \leftarrow X(k,a) : D(k,a,z,x) = 1]$$

Secure computation

Fix a (randomized) function f taking n inputs & producing n outputs

(inputs induce a distribution on outputs)



$$f(x_1, \ldots, x_5) = (y_1, \ldots, y_5)$$

Correctness

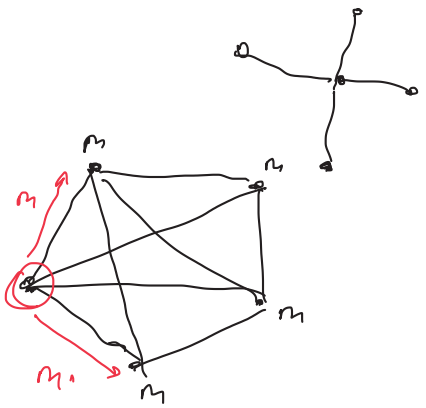
How to define security? correctness, privacy

- real/ideal paradigm — real-world execution should be "close" to ideal
- define real world
- define ideal world
- define notion of "closeness"

real world:

- communication model
  - broadcast?
    - synchrony? (rushing)
    - complete graph?
    - secrecy/integrity?
- setup?
- corruptions — how many?
  - adaptivity?
  - passive/active? fail-stop

semi-honest → malicious



ideal world
- define an appropriate functionality
- corruptions

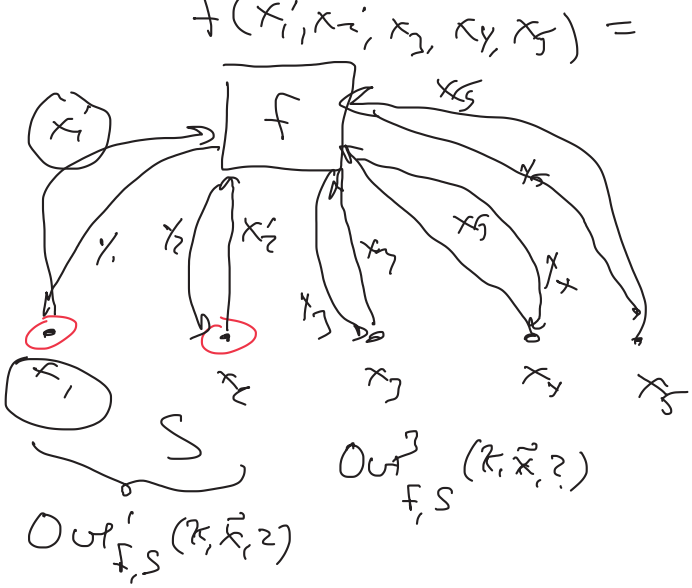
---

real-world execution defined by a protocol Π w/ adversary A
- passive adversary follows protocol
- active adversary behaves arbitrarily

$\text{Real}_{\Pi,A}(k, \vec{x}, z)$ — $\text{View}^A_{\Pi,A}(k, \vec{x}, z)$ $\quad (\text{Out}^1_\Pi(k), \text{Out}^2_\Pi(k))$

$\text{Out}^i_{\Pi,A}(k, \vec{x}, z)$

ideal-world computation of f
- input substitution
- computation
- output
- aborting?



$\text{Ideal}_{f,S}(k, \vec{x}, z)$ $\quad \text{Out}^2_{f,S}(k, \vec{x}, z)$

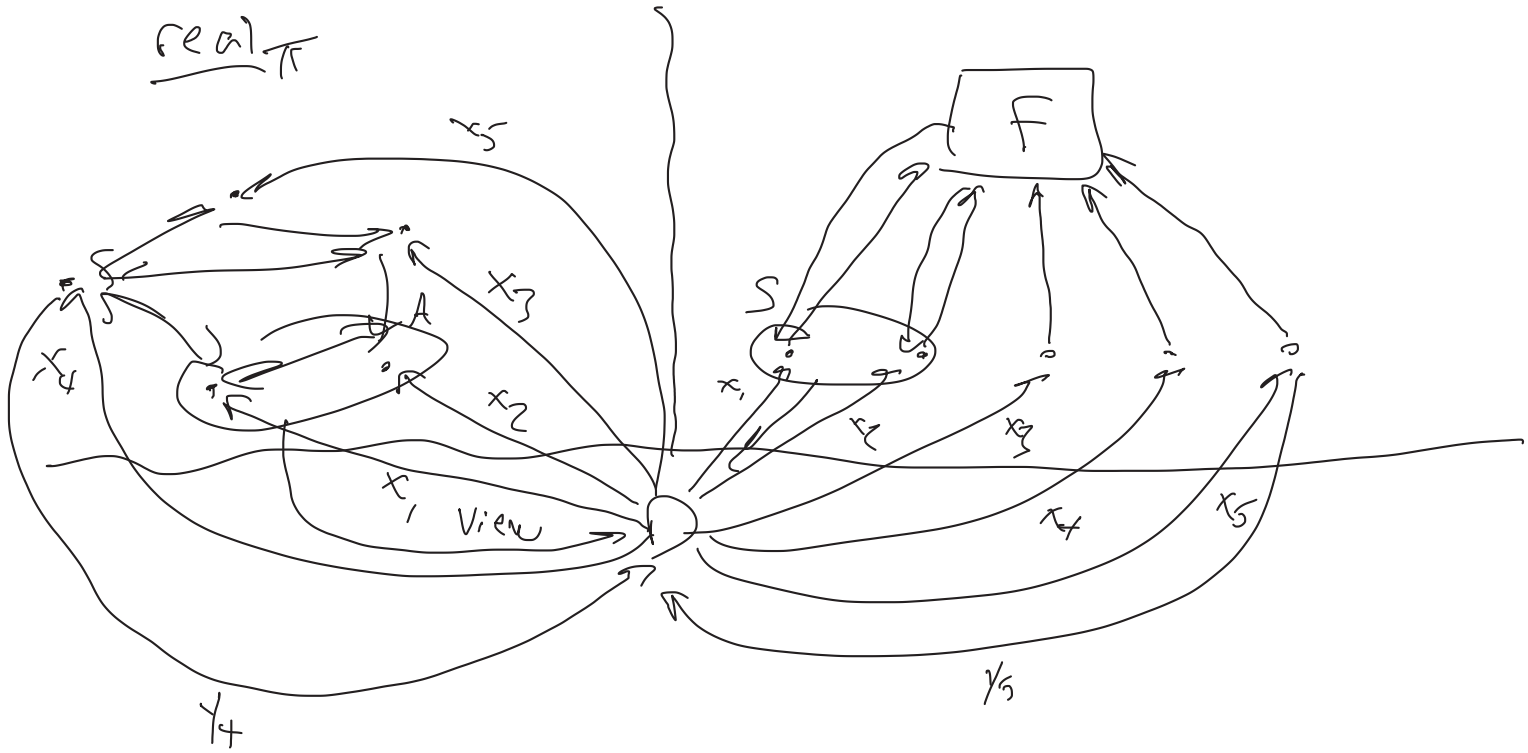
$\text{Out}^1_{f,S}(k, \vec{x}, z)$

Defining security:

Protocol Π is t-secure if for all prob. poly-time (PPT) adversaries A corrupting at most t parties, $\exists$ poly-time S corrupting at most t parties s.t.

$$\{(\text{View}_{\Pi,A}(k, \vec{x}, z), \text{Out}^H_{\Pi,A}(k, \vec{x}, z))\} \approx$$

$$\{(\text{Out}^S_{f,S}(k, \vec{x}, z), \text{Out}^H_{f,S}(k, \vec{x}, z))\}$$



$f(\cdot,\cdot) \to (r, \perp)$