CSci 8271
Security and Privacy in Computing
Day 3: Metal: Metadata-hiding file sharing

Stephen McCamant

University of Minnesota

Homomorphic encryption

- Many public-key encryption primitives allow some operation to be done on a ciphertext
  - E.g., in plain RSA, product of encryptions is the encryption of the product
- Not always helpful, but good for building fancier crypto applications
- Encryption-key-only rerandomization is a related feature

Secure multiparty computation

- Idea: Alice and Bob compute a function $f(a, b)$ of their respective private inputs a and b
  - They learn the function output but nothing else about the other's input
- Now a well-establish capability, but more expensive and restricted than having a trusted third party

Oblivious transfer

- Basic block of MPC and other crypto protocols
- A has two values. B receives one of his choice, but A doesn't know which
- Can be built on top of public-key crypto, seemingly not just symmetric

Garbled circuits (1/2)

- The classic scheme (Yao) for semi-honest S2PC, assuming the function is a Boolean circuit.
- Alice generates an encrypted circuit representation:
  - For each wire, 0 and 1 are labeled by random strings
  - Each 2-input gate is a 4-row lookup table
  - For each row, encrypt output label with input labels as keys; shuffle rows
  - Alice sends Bob encryptions of her inputs

Garbled circuits (2/2)

✓ Alice generates an encrypted circuit representation

- Bob has Alice encrypt his inputs via oblivious transfer
- Bob evaluates the circuit gate by gate
- Costs/limitations: space blowup, network traffic, sharing results, Alice honesty

Secret sharing

- Suppose I want to give a secret value s to two people, but they can only use it if they work together
- Classic approach: generate random r, send $s \oplus r$ to one person and r to the other
- Generalizes to "threshold" mechanisms (e.g., t out of n people) and for other primitives

Honest-but-curious

- AKA "semi-honest": most optimistic common assumption short of a party being completely trusted
- Party will follow the rules of the protocol, but might try to infer other information from what they see
- Useful as a stepping stone in exploring what's possible
- Arguably almost as hard to depend on as full trust in the real world