Statistical Database Security

Doug Tygar (doug.tygar@gmail.com)

November 2, 2005

cs161.org

Last lecture

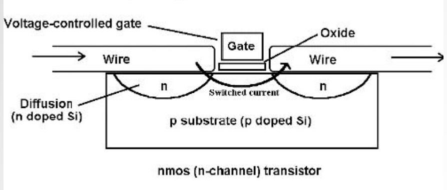
- Covert channels
- Two types of leaked information
  - Covert channels (deliberate)
  - Side channels (accidental)

Side channel examples

- Sound of keyboard typing
- Timing
- Power attacks

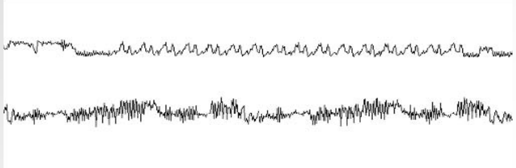
Power Analysis

Figure: Typical MOS Transistor in an IC



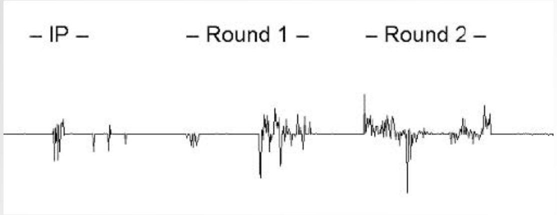
Simple Power Analysis

- Top line (DES)
- Bottom line (one cycle of DES)



Differential Power Analysis

- Repeat, and look for statistical averaging



Shamir secret sharing

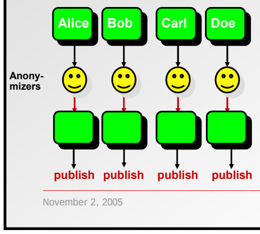
- How did this work

Adding with Shamir secret sharing

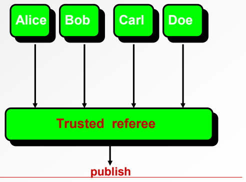
- Suppose we want to find everyone's average salary

Unsatisfactory solutions to puzzle

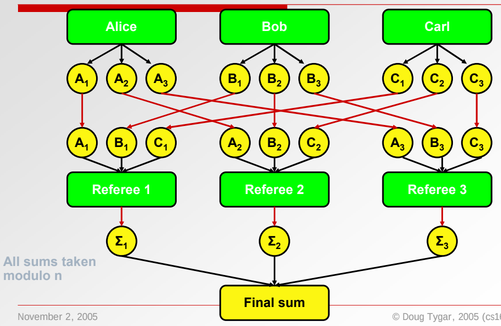
- Mix approach:
  - Everyone sends salary anonymously to third parties who publish



- Escrow approach:
  - Everyone sends salary to trusted escrow agent



Using Shamir Secret Sharing



Census bureau problem

- Wants to publish average statistics
- But how do they change when a new person joins?

Approaches that don't work

- Adding noise
  - Why not?
- Thresholding
  - Why not?