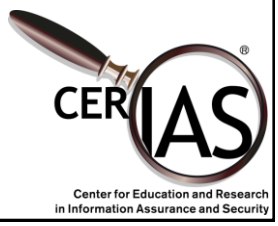
PURDUE UNIVERSITY

CS42600: Computer Security

Cryptographic Protocols

Prof. Chris Clifton

5 February 2019



PURDUE UNIVERSITY

Uses of Cryptography

- Ensuring Confidentiality
  - Chaining
- Verifying Integrity
  - Digital Signatures
- Verifying Identity
  - Certificate Authorities
- Establishing Communication
  - Key exchange
- Computing Without Revealing Data
  - Homomorphic Encryption
  - Secure Multiparty Computation
- Unforgeable Computations
  - Digital Cash
- *And many more*
  - *Some we haven't thought of yet*

2

Cryptographic Protocols

- Assumption: Cryptography / Ciphers / Hashes that satisfy certain properties
  - Indistinguishability, IND-CPA, IND-CCA, …
  - Separate encryption/decryption keys
  - Homomorphic: $D(E(A) \circ E(B)) = D(E(A+B))$
  - Typically assume block-level encryption
- Given these, build protocol that does more
  - Chaining (CBC, CTR)
  - Digital Signatures

4

Challenge: Ensuring *Protocol* Secure

- Failures typically not "breaking crypto"
  - Instead, identify flaws in the protocol using crypto
- Types of flaws
  - Implementation (software vulnerability)
  - Design flaws (protocol inherently insecure)
  - Mismatch between crypto properties and protocol assumptions

5

PURDUE UNIVERSITY

Secure Multiparty Computation

- Multiple parties 1, 2, 3, 4 each have data D_1, D_2, D_3, D_4
- Want to compute $R = f(D_1, D_2, D_3, D_4)$
- Don't want to reveal their own data
- What does "not reveal their own data" mean?
  - Suppose $f(x) = x$?
- Answer: "Ideal" vs. "Real" model
  - Ideal model captures desired outcome

PURDUE UNIVERSITY

What is SMC?
Ideal Model: Trusted Third Party

PURDUE UNIVERSITY

Don't Need the Third Party! Simple Example: Secure Sum

- Is plane within weight limit?
  - Need to know Σ weight

75-R = $w_{c+}w_{m+}w_{j+}w_b$

?'+w_b

w_c+R

-387+w_m

?+w_j

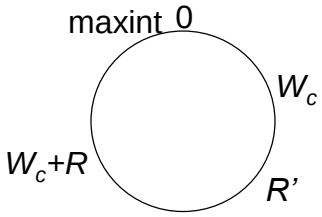
PURDUE UNIVERSITY

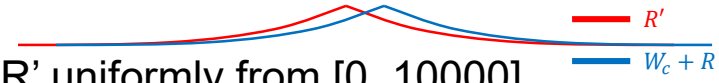
Prove Security

- Demonstrate that outcome in real model equals outcome in ideal model
  - If a party gets information in the real model, they could learn the same thing in the ideal model
- Secure Sum:
  - In real model, Mummoorthy learns W_c+R
    - Can he learn this in Ideal model?
  - Prove that Mummoorthy can *simulate* W_c+R

Idea: Value follows Distribution

- W_c+R is a different value every time, even if W_c unchanged
- Simulator selects a random R'
  - Won't be the same as W_c+R
  - But does it follow the same distribution?





- Select R, R' uniformly from [0, 10000]
  - *Still not good enough*

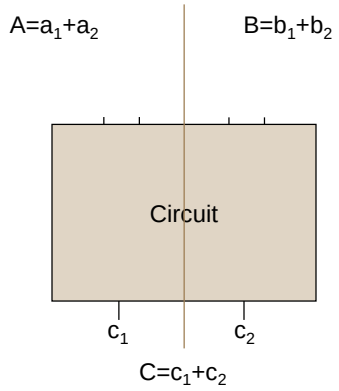
Steps to a Secure Protocol

- Define what it means to be secure
  - Prove that this satisfies what we want it to mean
  - *Often general methods exist*
- Develop protocol
  - Identify properties satisfied by primitives used
  - Prove that it gives desired result
    - *Using only the satisfied properties*
  - Prove that it satisfies security definition
- Implement carefully
  - And get others to inspect the code

PURDUE UNIVERSITY

Secure Multiparty Computation: Generic Solution

- Each side has input, knows circuit to compute function
- Add random value to your input, give to other side
  - Each side has share of all inputs
- Compute share of output
  - Add results at end
- XOR gate: just add locally
- AND gate: send your share encoded in truth table
  - Oblivious transfer allows other side to get only correct value out of truth table



value of (a_2,b_2)	(0,0)	(0,1)	(1,0)	(1,1)
OT-input	1	2	3	4
value of output	$c_1+a_1b_1$	$c_1+a_1(b_1+1)$	$c_1+(a_1+1)b_1$	$c_1+(a_1+1)(b_1+1)$

PURDUE UNIVERSITY

Digital Currency

- Desired properties: Unique Token that
  - Can't be duplicated
  - Can't be forged
  - Can't be stolen
- How do we formalize the desired properties?
  A. Mine Bitcoin
  B. Read the Bitcoin definition
  C. Define in Ideal model
  D. Construct a Blockhain

14

PURDUE UNIVERSITY

Common Protocol Mistakes

Simple to Exploit

- Deterministic Encryption
  - *E(A) = E(A)*
- Poor Diffusion
  - Fails if Eve has an idea of what might be sent
- Replay

Complex to Exploit

- Side-channel attacks
  - Timing:
    E(A) takes longer than *E(B)*
  - Padding oracle
  - Compression
- Man-in-the-middle
- Weak random numbers

16

PURDUE UNIVERSITY

Biggest Crypto Mistakes

- Failing to use it!
- Inventing your own
- Poor key management
  - Hard-coded keys
  - Keys stored with data
- No recovery plan

17