# Zero-knowledge Proof & Case study: How Real-world Crypto Systems Break

***Dawn Song***

***dawnsong@cs.berkeley.edu***



## Review

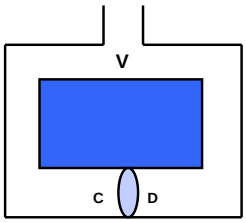
- **Secret sharing**
- **Zero-knowledge proof**



## Outline

- **Zero-knowledge proof**
- **Case study: how real-world security systems break**

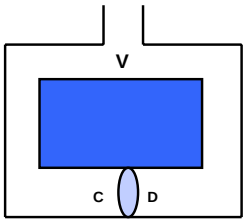
## The Zero-knowledge Cave (II)




1. Alice walks to either C or D;
2. Bob stands at V, calling either Left or Right;
3. Alice complies, using her magic word to open door if needed;
4. Alice & Bob repeats steps 1-3 for n times



## The Zero-knowledge Cave (III)




- What if Alice didn't know the magic word?
- What does Bob learn at the end of the proof?



## How to prove knowledge of square root

- Finding square root mod N=pq is as hard as factoring
- A knows b s.t. $b^2 =: y \mod pq$, & wishes to prove to B that she knows such b.
- A → B: $s =: r^2 \mod pq$ (A picks random r mod N)
- B flips coin
- B → A: coin flip
- If heads
  - A → B: $t =: r \mod pq$
  - B verifies $t^2 \equiv s \mod pq$
- If tails
  - A → B: $t =: rb \mod pq$
  - B verifies $t^2 \equiv sy \mod pq$
- What if A didn't know the square root?
- What did B learn after the proof?

## Administravia

- **HWs**
  - **Newsgroup posts on hws should only be clarification questions**
- **Office hours & feedback**
- **Late policy**
  - **20% off for 1 day delay**



## Things We've Learned So Far

- **Building blocks**
  - **Encryption, Hash, MAC, Digital Signature, etc..**
  - **How to generate random numbers**
  - **Secret sharing**
  - **Zero-knowledge proofs**
- **Use building blocks to build more advanced crypto-systems**
  - **Extremely trickly**
  - **Many real-world crypto systems are broken**
    - » **Weak design**
    - » **Wrong assumptions**



## Case Study: How to Break Real-world Crypto Systems

- **How to steal cars and get gas for free?**
- **How to break into "secure" wireless communication?**

## Steal cars with a laptop

- In April '07, high-tech criminals made international headlines when they used a laptop and transmitter to open the locks and start the ignition of an armor-plated BMW X5 belonging to soccer player David Beckham, the second X5 stolen from him using this technology within six months.
- … Beckham's BMW X5s were stolen by thieves who hacked into the codes for the vehicles' RFID chips …



## Digital Signature Transponder (DST)

- RFID tag, by Texas Instruments
- Used in car keys for vehicle immobilizers & keyless entry, gas cards, etc.
- 40-bit key
- Kaiser Cipher reverse engineered by researchers
- Exhaustiv search attack
  - Software implementation: may take 2 weeks to crack a key
  - FPGA implemenation: 21 hrs
  - 16-FPGA parallel attack: crack 5 key challenges from TI in 2 hrs



## Intercepting Mobile Communications: Breaking 802.11

- Original WEP protocol
  - Goal: protect communication btw access point & mobile station
  - Weak security design
- Message encrypted with RC4 with CRC checksum
  - IV is 24 bit
  - C = RC4(IV, k) ⊕ (m || CRC(m))
- Passive attack: decrypt traffic
- Active attack:
  - Modify traffic
  - IP redirection attacks to redirect traffic