Lecture 0: Some Odd Problems in Cryptography

Viet Tung Hoang
Agenda

1. The dating problem

2. Telephone coin flipping
The Dating Problem

**Issue:** Embarrassing if one wants a second date while the other doesn’t.
The Dating Problem

Privacy: Each person only knows:

1. His/her choice
2. The final outcome
3. Whatever can be inferred from (1) and (2).
Privacy for the Dating Problem

From Alice’s perspective:

Agree

-Alice knows that Bob agrees to date
Privacy for the Dating Problem

From Alice’s perspective:

Disagree

- Alice must not know whether Bob agrees to date or not
- Save Bob’s face if he actually agrees to date
Privacy for the Dating Problem

From Alice’s perspective:

-Alice knows that Bob doesn’t agree to date
-But Bob doesn’t know that Alice agrees → Save Alice’s face
How to Solve the Dating Problem: Step 1
How to Solve the Dating Problem: Step 2
How to Solve the Dating Problem: Step 3

Each takes turn to make a **private** cut
How to Solve the Dating Problem: Step 3

Each takes turn to make a **private** cut
If three ♥️ in a (wrap-around) row then date. Otherwise no date.
Why Is the Solution Correct?

There are ten ways to place 3 ♠️ and 2 ♣️ in a line.

For wrap-around, there are two groups.
The Initial Place

Date: Group 1

No Date: Group 2
Cutting Doesn’t Change the Group

Circular shift
Why Is the Solution Private?

Homework Exercise
Agenda

1. The dating problem

2. Telephone coin flipping
Telephone Coin Flipping

Alice and Bob want to decide who gets the car (over the phone)

Alice’s proposal:
• Alice tosses a coin and informs Bob of the outcome
• Bob gets the car if the coin lands head
Telephone Coin Flipping

Goal:
- Both Alice and Bob learn the outcome of a fair coin toss
- Nobody can cheat the other
A Physical Solution

Alice sends a random bit $M$ to Bob in a locked box

Bob sends another random bit $M'$ to Alice

Alice sends the key to Bob to open the box

Output $= M \oplus M'$
How to Implement A Digital Locked Box

First attempt:
- A locked box containing a bit $M$ is an encryption $C \leftarrow E_K(M)$
- The key to open the box is the key $K$

What can go wrong?
- Alice can send a fake key $K'$ so that $E_K^{-1}(C')$ is another bit of her choice
We Actually Need a **Bit Commitment Scheme**

**Commit:** \((C, K) \leftarrow \text{Comm}(M)\)

- committal
- \(M \in \{0, 1\}\)

**Decommit:** \(M' \leftarrow \text{DeComm}(K, C)\)

- \(M' \in \{0, 1\} \cup \{\perp\}\)

**Correctness:** If \((C, K) \leftarrow \text{Comm}(M)\) then \(\text{DeComm}(K, C) = M\)
Security Requirements of Bit Commitment

**Hiding**: Committal $C$ reveals **nothing** about $M$

Bob can’t learn the value in the locked box
Security Requirements of Bit Commitment

**Binding:** It’s **hard** to find $C^*$, $K_0$, $K_1$ such that
$\text{DeComm}(K_0, C^*) = 0$ and $\text{DeComm}(K_1, C^*) = 1$

Alice can’t construct a box that she can open to both 0 and 1
A Simple Bit Commitment Scheme

Commit to 0:
- Pick two 1024-bit primes $p$, $q$ such that:
  \[
  \begin{align*}
  p < q \\
  p \equiv 3 \pmod{4}, \; q \equiv 1 \pmod{4}
  \end{align*}
  \]

Commit to 1:
- Pick two 1024-bit primes $p$, $q$ such that:
  \[
  \begin{align*}
  p < q \\
  p \equiv 1 \pmod{4}, \; q \equiv 3 \pmod{4}
  \end{align*}
  \]

Committal: $N = pq$

Key: $(p, q)$