**CS 333: Network Security and Defense**

**Game of Like - Advanced Version**

# 1 Introduction

This in-class game is mainly used to engage students in class, and help students to understand public key and private key. More specifically, this game shows how to do a computation without exposing the input. Output: public, Input: private.

# 2 Problem

Alice and Bob just had their first date. Now they want to know if there is a second date or not. A problem happens if one party wants to go on a second date but the other party doesn't.

The Game of Like solves this problem; now a new problem arises - what if Alice cheats?

# 3 Solution

The solution is to play this advanced version of "game of like", a game that allows Bob to catch Alice cheating or vice versa. Still this game should not reveal the inputs - when one party says no, this party will not the other party's choice.

- One red ace left on the table, face down.
- Bob gets one red ace and one black ace.
- Alice gets eight cards: two black aces; two red aces, two black queens, two red queens.
- Bob puts his cards face down to the right of the open card.
- Alice needs to make two turns.
- Alice puts her cards face down to the left of the open card. She also puts one queen to the left of her aces.
- For Bob and Alice: a red ace next to the central card means like. However, Alice's queen has a special meaning later on, they will open Alice's queen later on: if it was red, they proceed as normal. If it was black, they change the order of two other Alice's cards (without looking, of course).
- Bob is allowed to choose one of two Alice's moves at random and open the two main cards of that move to make sure that both cards have the correct orientation. Bob will not see the corresponding queen, hence seeing the main cards will not disclose Alice's input.

- The three cards of that turn are discarded, the queen of the remaining turn is opened, the order of the cards is changed (if needed).
- Alice and Bob collect the five cards and take turn cutting the deck - cyclic shift only.
- They open the cards in order in a circle: if the three red aces or the two black aces are adjacent, they like each other.
- Nothing is revealed when the queens are not adjacent: it is unknown whether they both don't like each other or whether one does and one doesn't.

## 4 Reference

Tal Rabin of IBM Technion-Israel Institute of Technology lecture at Technion Computer Engineering 2014 summer school. https://www.youtube.com/watch?v=N0tsxHoIcWQ

Playing Card Cryptography, by Konstantin: http://fouryears.eu/2015/03/09/playing-card-cryptography/