TD 2 Advanced cryptography 2024

Léo Colisson Palais

Exercice 1: Ready?

Alice and Bob have been together for a while, and are thinking to marry. However, both of them are afraid to do their proposal as the other might refuse. They design instead the following protocol to reveal if both of them want to marry, without revealing anything else. They only have with them a few cups (indistinguishable and opaque), and some colored marbles (black and red, also indistinguishable except for the color). Then:

- If Alice wants to marry, she will hide a black marble under a flipped cup, and a red marble under a second cup placed to the right of the first cup. Otherwise, she will exchange the two marbles (i.e. red comes first, then black).
- Then, a red marble will be hidden under a cup, placed to the right of Alice's cups.
- Next, if Bob wants to marry, he will hides a red marble under a cup (again placed to the right of other cups), followed by a black marble hidden under a cup placed to the right of the first cup. Otherwise, he will exchange the two marbles (i.e. black comes first, then red).
- At that step, we have therefore 5 flipped cups placed on a line with one marble hidden behind each cup. To ease the following operations, the parties organize them into a circle, keeping the original ordering along the circle (the first cup will be next to the last one).
- While Bob is away, Alice will then randomly rotate the circle of cups.
- While Alice is away, Bob will also randomly rotate the circle of cups.
- At the end, all cups are removed, revealing the marbles.

1. How can Alice and Bob know if both of them want to marry while only looking at the marbles?
2. Describe the ideal functionality $\mathcal{F}$ that this protocol tries to realize.
3. Show that if Alice (resp. Bob) does not want to marry, then Alice (resp. Bob) learn no information regarding the choice of Bob (resp. Alice).
4. Show that if Alice wants to marry, then she can learn the choice of Bob. Is it possible to design a different protocol realizing $\mathcal{F}$ where this is not possible?
5. Unfortunately, Alice and Bob lost all their marbles. Instead, they want to replace them with cards, taking black cards instead of black marbles, and red cards instead of red marble (cups are then not useful anymore, they can hide the color by flipping the card). Is this still secure?
6. The above protocol is in fact computing a logical AND. Find a similar protocol that would instead compute a XOR.

Exercice 2: Poorly garbled circuit

1. Alice and Bob decide to run the garbled circuit protocol, but they choose the labels of the wire incrementally (first wire is labeled 1, second wire is labeled 2). Is this secure, and if not who can exploit this and how.
2. Instead, they sample the labels in $\{0,1\}^l$ for some l, function of the security parameter λ. Which of the following choices is good, bad, and why?
   - $l = \log(\lambda)$
   - $l = \lambda$
   - $l = 2^\lambda$