Security Protocols and Applications
(Part 1)

Final Exam
June 18th, 2009
Duration: 3:45

This document consists of 8 pages.

Instructions

Electronic communication devices and documents are not allowed.

This exam contains 2 independent parts.

Answers for each part must be written on its separate sheet.

Answers can be either in French or English.

Questions of any kind will certainly not be answered. Potential errors in these sheets are part of the exam.

You have to put your full name on the first page and have all pages stapled.
1 Coin Flipping over a Quantum Telephone

Alice and Bob are getting a divorce. They can’t stand facing each other but they have to discuss who gets the car. Since they don’t seem to agree about it, they finally decide to flip a coin. The problem is that they don’t trust each other. Fortunately, they attended to the “Security Protocols and Applications” class and have learnt oblivious transfer. We assume that they can use a quantum telephone (in addition to a classical one) so that they have an oblivious transfer channel at disposal. Concretely, Alice can send a bit through this special OT channel. Bob will receive this bit with probability $\frac{1}{2}$ and a special symbol $#$ otherwise.

1. In the case of oblivious transfer, explain what is the security property against a malicious Alice.

Explain what is the security property against a malicious Bob.
2. We consider the following game:

1. Alice flips a bit \( b_A \)
2. Bob flips a bit \( b_B \)
3. Alice sends \( b_A \) through the OT channel
4. Bob sends \( b_B \) to Alice (through a regular channel)
5. Alice sends \( b_A \) to Bob (through a regular channel)
6. If Bob did not receive the special symbol \( \# \) from the OT channel, he checks that the two received bits are equal. If this is not the case, Bob wins
7. Otherwise, Alice wins iff the two exchanged bits are equal

If Alice and Bob follow the rules of the game, what are the winning probability of Alice and Bob?

Propose a cheating strategy for Alice. What is its success probability when Bob is honest?

Propose a cheating strategy for Bob. What is its success probability when Alice is honest?
3. We consider the following game:

1: Alice flips bits $b_A, b_1, \ldots, b_{n-1}$ and sets $b_n = b_A \oplus b_1 \oplus \cdots \oplus b_{n-1}$
2: Bob flips a bit $b_B$
3: for $i = 1$ to $n$ do
4: Alice sends $b_i$ through the OT channel
5: Bob receives either $b'_i = b_i$ or a special symbol $b'_i = \#$
6: end for
7: Bob sends $b_B$ to Alice (through a regular channel)
8: Alice sends $b_A, b_1, \ldots, b_n$ to Bob (through a regular channel)
9: for $i = 1$ to $n$ do
10: if $b'_i \neq \#$ and $b'_i$ is not equal to the corresponding bit $b_i$ then the game stops and Bob wins
11: end for
12: if $b_A \neq b_1 \oplus \cdots \oplus b_n$ then the game stops and Bob wins
13: Alice wins iff $b_A = b_B$

If Alice and Bob follow the rules of the game, what is the winning probability of Alice and Bob?

Propose a cheating strategy for Alice. What is its success probability when Bob is honest?
Show that when Alice is honest, there is no cheating strategy for Bob to get any advantage with probability at least $1 - 2^{-n}$. 
4. We consider the following game:

1: Alice flips bits $b_A, b_{1,1}, \ldots, b_{m,n-1}$ and sets $b_{i,n} = b_A \oplus b_{i,1} \oplus \cdots \oplus b_{i,n-1}$ for $i = 1, \ldots, m$
2: Bob flips a bit $b_B$
3: for $i = 1$ to $m$ do
4: for $j = 1$ to $n$ do
5: Alice sends $b_{i,j}$ through the OT channel
6: Bob receives either $b_{i,j}' = b_{i,j}$ or a special symbol $b_{i,j}' = \#$
7: end for
8: end for
9: Bob sends $b_B$ to Alice (through a regular channel)
10: Alice sends $b_A, b_{1,1}, \ldots, b_{m,n}$ to Bob (through a regular channel)
11: for $i = 1$ to $m$ do
12: for $j = 1$ to $n$ do
13: if $b_{i,j}' \neq \#$ and $b_{i,j}'$ is not equal to the corresponding bit $b_{i,j}$ then the game stops and Bob wins
14: end for
15: if $b_A \neq b_{1,1} \oplus \cdots \oplus b_{i,n}$ then the game stops and Bob wins
16: end for
17: Alice wins iff $b_A = b_B$

If Alice and Bob follow the rules of the game, what is the winning probability of Alice and Bob?

Show that when Alice is honest, there is no cheating strategy for Bob to get any advantage with probability at least $1 - m2^{-n}$. 
Show that when Bob is honest, any cheating strategy for Alice makes her be caught red handed with probability at least $1 - 2^{-m}$.

5. Show that we can achieve bit commitment using oblivious transfer.
Any attempt to look at the content of these pages before the signal will be severely punished.

Please be patient.