LASEC

Family Name: ....

First Name: ....

Section: ....

Security Protocols and Applications (Part 1) — Solutions

Final Exam

June 18th, 2009

Duration: 3:45

This document consists of 8 pages.

Instructions

Electronic comunication 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.

   > *A malicious Alice shall not be able to know what Bob has received. She shall not be able to influence the probability of reception either.*

   Explain what is the security property against a malicious Bob.

   > *A malicious Bob shall not be able to know what Alice has sent in the case he receives #. He shall not be able to influence the probability of reception either.*

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?

   $\Pr[b_A = b_B] = \frac{1}{2}$ *so Alice and Bob have a fair probability of winning.*

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

   At Step 5:, Alice sends the received b_B instead of b_A.
   If Bob receives # from the OT channel, the probability is 1. Otherwise, the probability is $\frac{1}{2}$. Thus, the winning probability is $\frac{3}{4}$.

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

   At Step 4:, if Bob did not receive # then he sends the received $1 - b_A$ instead of b_B.
   If Bob receives # from the OT channel, the probability is $\frac{1}{2}$. Otherwise, the probability is 1. Thus, the winning probability is $\frac{3}{4}$.

3. We consider the following game:

```
1: Alice flips bits b_A, b_1, ..., b_{n-1} and sets b_n = b_A ⊕ b_1 ⊕ ··· ⊕ 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, ..., b_n to Bob (through a regular channel)
9: for i = 1 to n do
10:    if b'_i ≠ # 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 ≠ b_1 ⊕ ··· ⊕ 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?

$\Pr[b_A = b_B] = \frac{1}{2}$ *so Alice and Bob have a fair probability of winning.*

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

At Step 8:, Alice sends the received b_B instead of b_A. If different, she flips one b_i selected at random. *If $b_A = b_B$, the probability of success is 1. Otherwise, the probability is the probability that the flipped b_i was not received from the OT channel, which is $\frac{1}{2}$. Thus, the winning probability is $\frac{3}{4}$.*

Show that when Alice is honnest, there is no cheating strategy for Bob to get any advantage with probability at least $1 - 2^{-n}$.

With probability $1-2^{-n}$, there is at least one b_i which is not received by Bob. If Bob decides to send a bit b at Step 7:, the probability that $b \neq b_A$ is the probability that $b = b_1 \oplus \cdots \oplus b_n$. Since all b_j's are independent and one b_i is missing for Bob, this probability is $\frac{1}{2}$ so Bob has no advantage.

4. We consider the following game:

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 $i = 1, \ldots, m$
Bob flips a bit b_B
for $i = 1$ to m **do**
  for $j = 1$ to n **do**
    Alice sends $b_{i,j}$ through the OT channel
    Bob receives either $b'_{i,j} = b_{i,j}$ or a special symbol $b'_{i,j} = \#$
  end for
end for
Bob sends b_B to Alice (through a regular channel)
Alice sends $b_A, b_{1,1}, \ldots, b_{m,n}$ to Bob (through a regular channel)
for $i = 1$ to m **do**
  for $j = 1$ to n **do**
    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
  end for
  if $b_A \neq b_{i,1} \oplus \cdots \oplus b_{i,n}$ then the game stops and Bob wins
end for
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?

$\Pr[b_A = b_B] = \frac{1}{2}$ *so Alice and Bob have a fair probability of winning.*

Show that when Alice is honnest, there is no cheating strategy for Bob to get any advantage with probability at least $1 - m2^{-n}$.

Thanks to the previous question, for each of the m iterations, Bob gets no advantage with probability at least $1 - 2^{-n}$. In total, Bob gets no advantage with probability at least $1 - m2^{-n}$.

Show that when Bob is honnest, any cheating strategy for Alice makes her be caught red handed with probability at least $1 - 2^{-m}$.

If Alice decides to flip b_A, she must keep the matrix of $b_{i,j}$'s consistent thus must flip at least one bit in each row. So she must flip at least m bits. The probability that she is not caught is the probability that each bit she has flipped was not received by Bob. This probability is at least 2^{-m}.

5. Show that we can achieve bit commitment using oblivious transfer.

The coin flipping protocol that we defined is actually a bit commitment scheme: Alice first commits on b_A, then Bob sends b_B, then Alice opens her commitment. More precisely, the commitment protocol works as follows:

***Commit to** b:*

Alice flips bits $b_{1,1}, \ldots, b_{m,n-1}$ and sets $b_{i,n} = b \oplus b_{i,1} \oplus \cdots \oplus b_{i,n-1}$ for $i = 1, \ldots, m$
for** $i = 1$ to m **do
    for** $j = 1$ to n **do
        Alice sends $b_{i,j}$ through the OT channel
        Bob receives either $b'_{i,j} = b_{i,j}$ or a special symbol $b'_{i,j} = \#$
    end for
end for

***Open commitment**:*

Alice sends $b, b_{1,1}, \ldots, b_{m,n}$ to Bob (through a regular channel)
for** $i = 1$ to m **do
    for** $j = 1$ to n **do
        if $b'_{i,j} \neq \#$ and $b'_{i,j}$ is not equal to the corresponding bit $b_{i,j}$ then the protocol aborts
    end for
    if $b \neq b_{i,1} \oplus \cdots \oplus b_{i,n}$ then the protocol aborts
end for

Any attempt to look at
the content of these pages
before the signal
will be severly punished.

Please be patient.