Introduction to Cryptography 4/27/18

Lecture 23: Secure Computation II

Instructor: Vipul Goyal *Scribe: Alexander Litzenberger*

1 Review

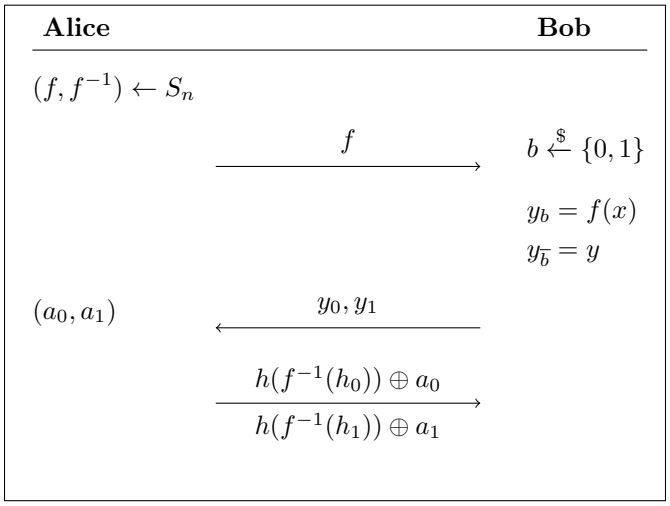
2 Oblivious Transfer

Definition 1 *(Oblivious Transfer) Oblivious transfer is a protocol in which a sender sends some subset of n pieces of information to a receiver but remains oblivious as to which subset has been sent.*

Definition 2 *(Semi-Honest Adversary) A semi-honest adversary is an adversary who correctly follows the protocol but will try to attack the transcript. I.E. Honest during protocol execution and malicious after the protocol.*

2.1 Scheme secure against semi-honest adversaries

The first construction is a 1-of-2 Oblivious Transfer in which both parties are semi-honest.



Note S_{2^n} is the symmetric group over 2^n I.E. the set of bijective functions from a set of 2^n symbols to itself.

Problems given Malicious Adversaries While this scheme does in fact succeed given the assumption of semi-honest adversaries it has shortcomings that cause it to fail against malicious adversaries.

1) If f is not a permutation then y_0, y_1 could leak B.

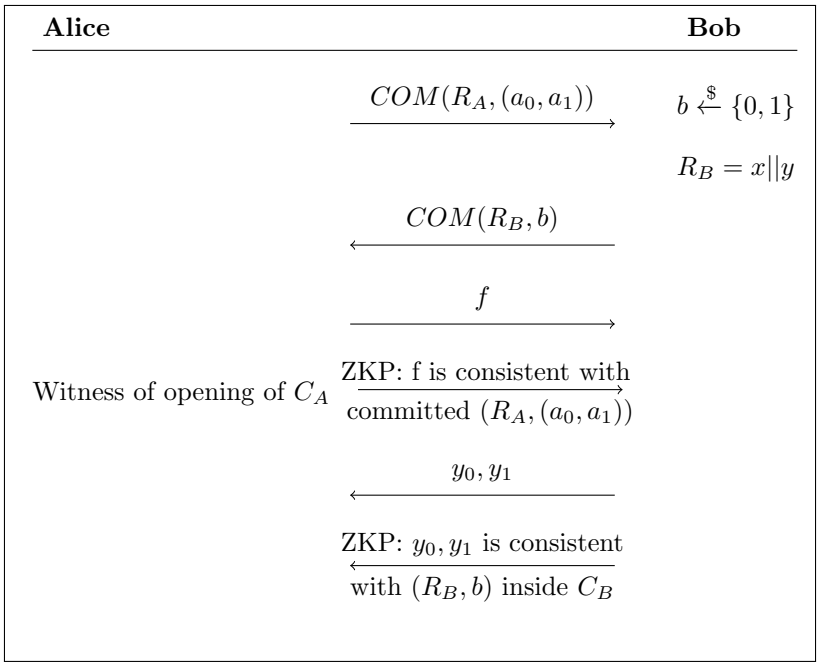
2) If B knows the preimage of both y_0, y_1, B could learn (a_0, a_1)

3 Goldreich-Micali-Wigderson Compiler (GMW Compiler)

The GMW compiler takes an arbitrary Oblivious Transfer scheme secure against semi-honest adversaries and Transforms it into one secure against Malicious Adversaries.

3.1 Attempt One

First we will attempt a construction following closely from the OT scheme above then analysis the concerns that remain. Note the Zero Knowledge Proofs (ZKPs) are in-fact multi-round protocols.



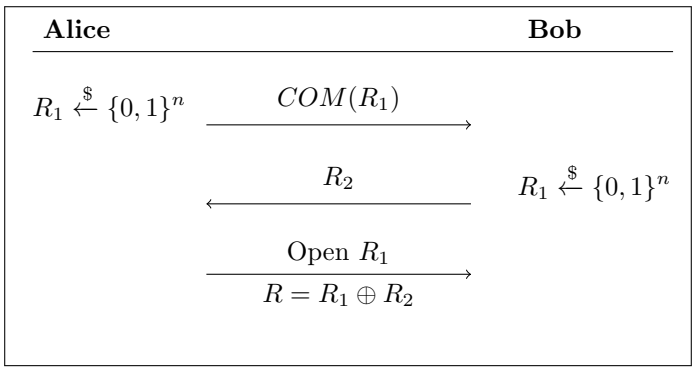
Concerns

1) Parties choose their randomness honestly.

2) Each message of the protocol is consistent with this randomness (and input)

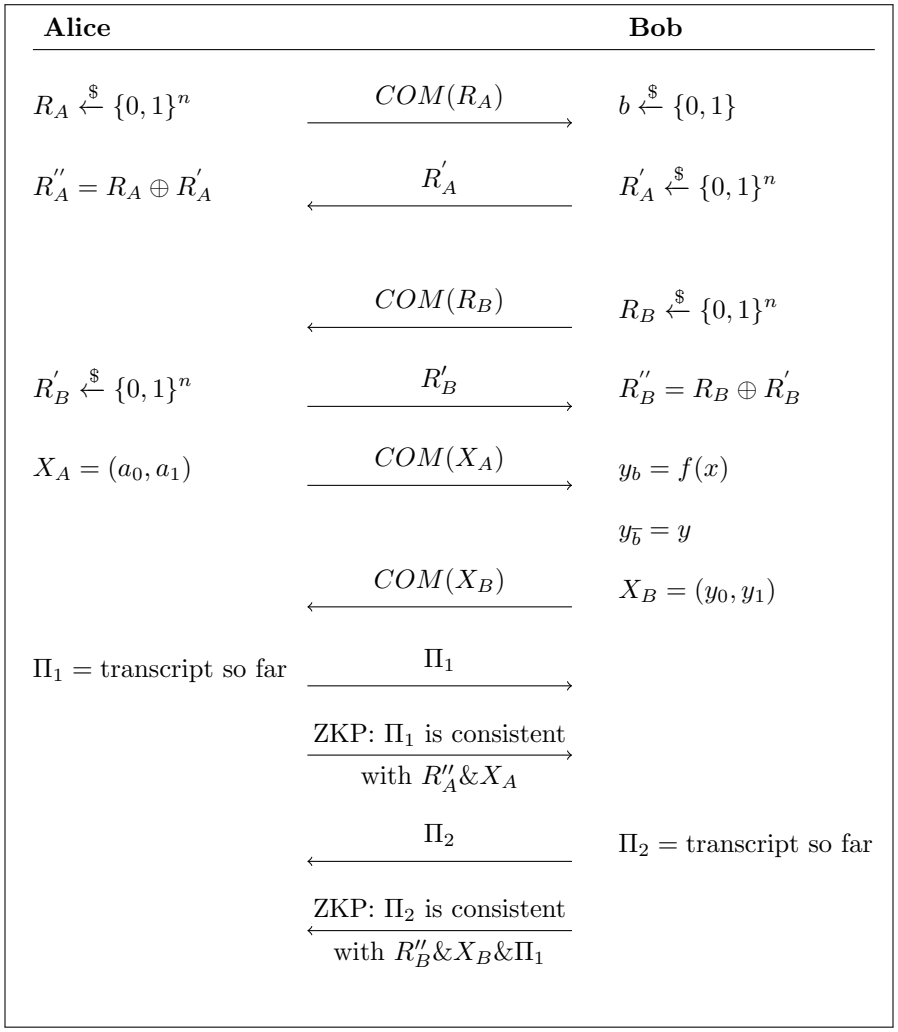
3.2 Detour on coin flipping:

Coin Flipping by Telephone is a protocol for establishing consensus on randomness between two parties without requiring them to trust the other party or verify their means of generating the randomness. A simple protocol for doing this follows.



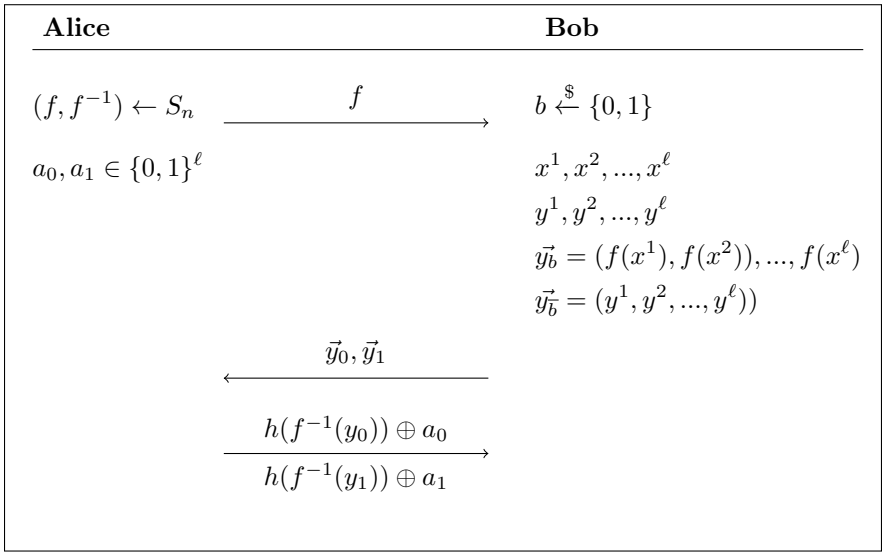
3.3 Attempt Two (Final)

Now using ideas from coin flipping we will address the above concerns and construct a full scheme for converting a OT scheme secure against semi-honest adversaries to one secure against malicious adversaries. The general notion is to make each party prove their honesty in a Zero-knowledge manner in all cases where they could potentially cheat, specifically by proving the values that are meant to depend on others in the transcript in fact do in the way the protocol being compiled prescribes.



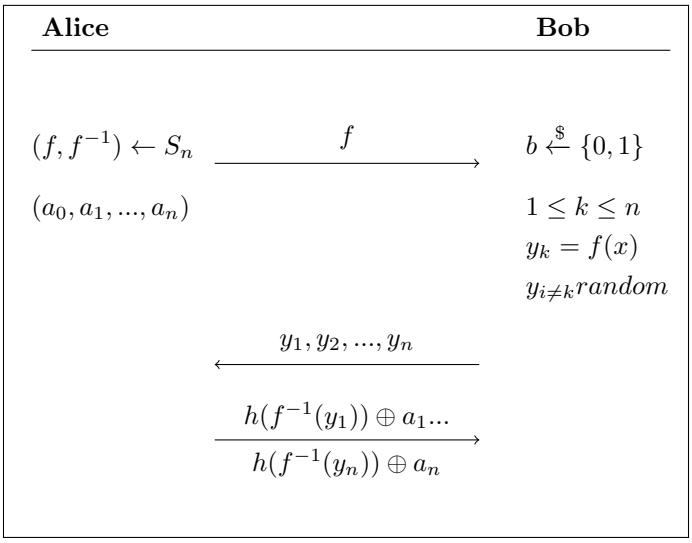
4 Going to string Oblivious Transfer (One-Out-of-Two OT)

Now that we have established the basics of OT we will now move on to extending the notion to more general forms of information to be transfered. First we will consider One-Out-of-Two Oblivious Transfer of strings.



5 Going to One-Out-of-N Oblivious Transfer (Bits)

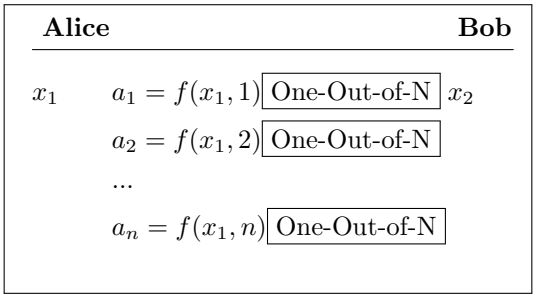
Now we will move on to One-Out-of-N Oblivious Transfer, note this scheme relies on the specific construction of One-Out-of-Two OT we have constructed above.



Claim: The above protocol can be extended to One-Out-of-N string Oblivious Transfer.

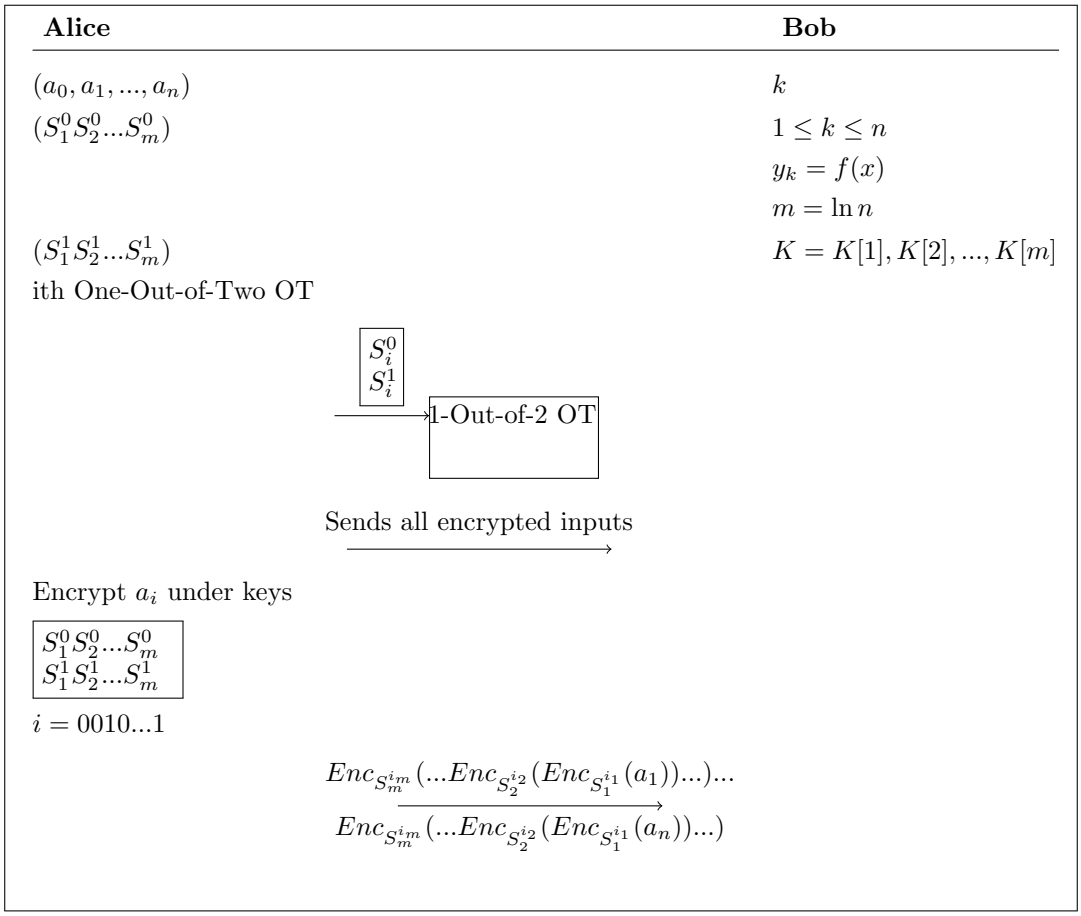
Lemma: One-Out-of-N Oblivious Transfer implies Multi-Party Computation for any circuit f as long as one of the inputs (x_1, x_2) is "small".

Proof: Say A and B want to compute $f(x_1, x_2)$



6 Generic Construction of One-Out-of-N Oblivious Transfer

Now we will consider another construction of One-Out-of-N Oblivious Transfer that does not depend on the specific construction of One-Out-of-Two Oblivious Transfer as the previous scheme did. This protocol will be constructed generically given a One-Out-of-Two Oblivious Transfer scheme.



That is m oblivious transfers of keys are done then each message is encrypted under a distinct set of keys with one from each of the One-Out-of-Two Oblivious Transfer rounds and then the messages are transmitted and Bob will have a set of keys exactly sufficient for decrypting one of the messages.