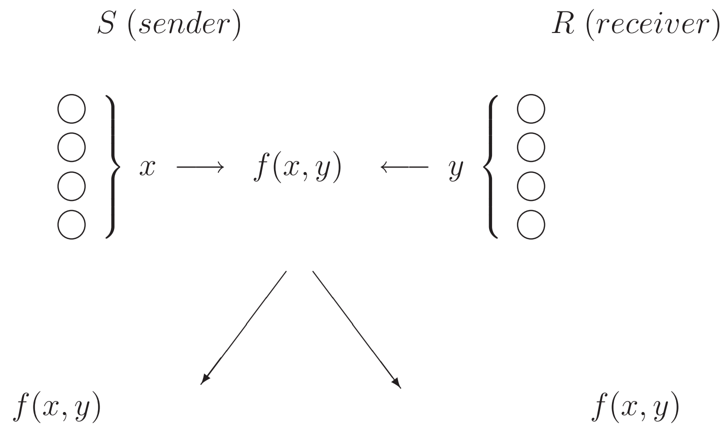
1 Lecture 10

2 Oblivious Transfer

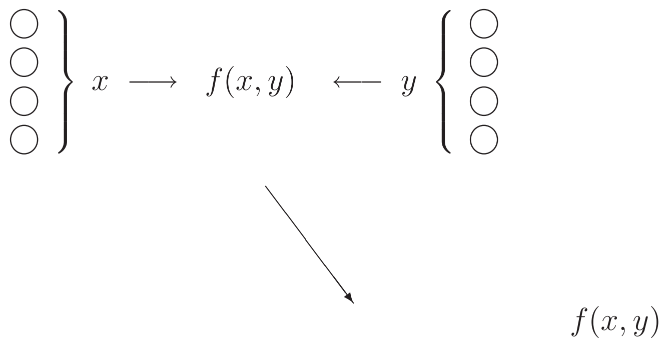
There are no more specific P and V. But we can use the notion of IP whenever we need it. The following examples give us a basic idea for oblivious transfer. We have a sender and a receiver in the following applications.



In this application, the symbol ”◯” represents that commits to some values. Both the sender and receiver can learn f(x, y). But the sender will not learn anything about the input y and the receiver will not also learn anything about the input x. f(x, y) is a function of x and y.

Suppose only R obtain f(x,y), the above figure will become:

S ($sender$) $\qquad\qquad$ R ($receiver$)



In this application, only the receiver learns f(x, y).

2.1 The definition of Oblivious Transfer

Now we can give the difinition of oblivious transfer:
An Oblivious Transfer is a process by which Alice sends to Bob a bit over a noisy channel without knowing whether it arrives.

The original obvilious transfer concept is introduced by Rabin.

The basic idea of Rabin OT can be described as the following:

$$\begin{array}{rcl} Alice & & Bob \\ m\ (message) & \longrightarrow & \begin{cases} get \quad m \quad with \quad prob.\ 1/2, \\ get \quad ? \quad with \quad prob.\ 1/2. \end{cases} \end{array}$$

Here, wiping out the message happens half of the time and so is the correct transmission of the message.

The following two examples describe one possible implementation of R-OT based on factoring::

Example 2.1

$$\begin{array}{rcl}
Alice & & Bob \\
m \;=\; p \,*\, q & \xrightarrow{\quad m \quad} & \\
 & & x \in_R Z_n^*, \\
 & & y \leftarrow x^2 \; mod \; n \\
 & \xleftarrow{\quad y \quad} & \\
x' \leftarrow \sqrt{y} \; mod \; n & & \\
 & \xrightarrow{\quad x' \quad} & \\
 & & \textbf{if } x = \pm x' \; (mod \; n), \textbf{then } get \; ? \\
 & & \textbf{else } compute \; p, \; q \\
 & & (x - x')(x + x') \equiv 0 \; (mod \; n). \\
 & & \Longrightarrow x^2 \equiv y^2 0 \; mod \; n.
\end{array}$$

Example 2.2

$$\begin{array}{rcl}
 & n = p * q & \\
 & e & \\
Alice & & Bob \\
 & \xrightarrow{\; m^e \; mod \; n \;} & \\
 & & x \in_R Z_n^*, \\
 & & y \leftarrow x^2 \; mod \; n \\
 & \xleftarrow{\quad y \quad} & \\
x' \leftarrow \sqrt{y} \; mod \; n & & \\
 & \xrightarrow{\quad x' \quad} &
\end{array}$$

Bob can factor n with probability 1/2 and then find out m.

However, we must have

$1/2 \leq Pr(Bob\ can\ factors) \leq 1/2 + 1/poly(|n|)$, for every polynomial. (**)
Moreover, we know:

fact: factoring $\Longleftrightarrow$ extracting square roots.
However, there could be a deterministic reduction.
$n \to\ y \to \sqrt{y} \to p,\ q.$ $\sqrt{y}$: factoring n.

In order to keep the property of (**), Alice has to make sure that y is really a square of some number, i.e. Bob really knows $\sqrt{y}$ and using zero-knowledge proof to prove Bob knows $\sqrt{y}$.

$$n = p * q$$

$$\begin{array}{ccc} Alice & & Bob \\ & & x \in_R Z_n^*, \\ & & y \equiv x^2 \ mod \ n \\ & \xleftarrow{y} & \\ & \xleftarrow{ZK\ (y \in QR_n)} & \\ x' = \sqrt{y} & \xrightarrow{x'} & \end{array}$$