Bonn-Aachen International Center for Information Technology
Cryptography and Game Theory — Raekow, Ziegler
IPEC Winter 2012

Scribe(s): Niclas Zimmermann — Lecture 3 & 4, Date: 13.03.2012

1 Cryptography

In this lecture we show first a protocol for secure multiplication. It will work for 3 parties. Later we will generalize our ideas of secure addition/multiplication for more parties and more general functions. In this sence we will discuss a *protocol for circuit evaluation* and give a definition of *Shamir's secret sharing*.

1.1 Secure Multiplication

The situation is that there are three parties (P_1, P_2, P_3). The first two parties possess values $a \in \mathbb{Z}_p$ and $b \in \mathbb{Z}_p$ (resp.). Without revealing a and b they want to compute the product $ab \mod p$. A protocol that achieves this is described in the following:

The starting position is:

$n = 3$

$P_1 : a \in \mathbb{Z}_p$

$P_2 : b \in \mathbb{Z}_p$

The protocol works as follow:

1.Split We split the values a and b randomly in a sum of three summands:

$$\begin{aligned} a &= a_1 + a_2 + a_3 \mod p \\ b &= b_1 + b_2 + b_3 \mod p \end{aligned}$$

2.Share The values a_i and b_i $(i = 1, 2, 3)$ are shared in this way:

P_1	P_2	P_3
a_2	a_1	a_1
a_3	a_3	a_2
b_2	b_1	b_1
b_3	b_3	b_2

Now P_1 knows a_2, a_3, b_2 and b_3, P_2 knows $a_1, \ldots$

3.Compute Now we let each party compute one of the three values u_1, u_2 and u_3:

P_1 computes	P_2 computes	P_3 computes
u_1	u_2	u_3
$\vdots$	$\vdots$	$\vdots$
a_2b_2	a_1b_3	a_1b_1
$+$	$+$	$+$
a_2b_3	a_3b_1	a_1b_2
$+$	$+$	$+$
a_3b_2	a_3b_3	a_2b_1

We can use the protocol secure addition (discussed earlier) such that that the players learn the sum $u_1 + u_2 + u_3$, but none of the summands u_1, u_2.

It is easy to see that $ab = a_2b_2+a_1b_3+a_1b_1+a_2b_3+a_3b_1+a_1b_2+a_3b_2+a_3b_3+a_2b_1 = u_1+u_2+u_3$. That means *correctness* is given.

Also *privacy* holds because each party knows only two shares of a value (a or b). So no party can compute more than one value u_i (he would need more shares). On the other hand no party knows the value u_i of another party as secure addition is privat.

1.2 Protocol for Circuit Evaluation

In general a protocol for MPC works in three steps:

1. Sharing
2. Local computation
3. Output reconstruction

Until now we have just discussed protocols for 3 players. Of course, we want to generalize the protocols of secure addition and secure multiplication for *more players*. But there is one more disadvantage that we do not want to keep. If two players collaborate they can learn additional informations. Now, if we have more than 3 players this would be poor. If $t < n/2$ adversaries get together after computation the protocol (*Shamir's secret sharing*) remains secure against semi-honest adversaries. We still assume that the (unbounded) adversaries follow the protocol.

1.2.1 Shamir's secret sharing

This protocol works for $n \geq 3$ parties. If we want to share a secret $s \in \mathbb{F}$ we choose randomly a polynomial $f_s \in_{\mathrm{R}} \mathbb{F}[X]$ with the following properties:

- $\deg(f_s) = t$
- $f_s(0) = s$

And we give to each player i a share $f_s(x_i)$ where $x_i \neq x_j$ for $i \neq j$. Usually we choose $x_i = i$. There are some basic facts:

- If one distributes fewer than t shhares, they do not certain information about s.

- If one distributes $t+1$ or more shares, then we can reconstruct the secret.

In order to compute $f_s(0)$ (which is the secret s) we pick $t+1$ values x_i and their shares $s_i := f_s(x_i)$. We can write

$$f_s(x) = \sum_i f_s(x_i) L_i(x)$$

where $L_i = \prod_{j \neq i} \frac{x - x_j}{x_i - x_j}$ are the Lagrange polynomials.

Now player i computes locally $w_i := s_i r_i$ where $r_i := L_i(0)$. When every player publish her value w_i the players can easily compute the secret

$$s = f_s(0) = \sum_i w_i = \sum_i s_i r_i = \sum_i s_i L_i(0).$$

Example. $P_1, \ldots, P_5$ want to tolerate $t = 2$ corrupted parties. We work in $\mathbb{F} = \mathbb{Z}_{23}$ and want to share the secret $s = 19$. So we choose two values $a_1, a_2 \in_{\mathrm{R}} \mathbb{F}$, say $a_1 = 9$ and $a_2 = 11$. That means our polynomial is

$$f_s(x) = s + a_1 x^2 + a_2 x + 19 = 11x^2 + 9x + 19 \mod 23.$$

Now we can compute the shares:

$$\begin{aligned} s_1 = &\quad f_s(1) &&= 16 \\ s_2 = &\quad f_s(2) &&= 12 \\ s_3 = &\quad f_s(3) &&= 7 \\ s_4 = &\quad f_s(4) &&= 1 \\ s_5 = &\quad f_s(5) &&= 17 \end{aligned}$$

We pick the values of P_3, P_4 and P_5. They compute $w_i = s_i \prod \frac{-x_j}{x_i - x_j}$:

$$\begin{aligned} w_3 &= 7\left(\frac{-4}{3-4}\right)\left(\frac{-5}{3-5}\right) = 1 \\ w_4 &= 8 \\ w_5 &= 10 \end{aligned}$$

It remains that we add them to each other

$$w_1 + w_2 + w_3 = 19 \mod 23.$$

And in this way the parties know the secret.

1.2.2 Arithmetic circuits

The MPC protocol is secure against semi-honest adversaries. The number of players is $n \geq 3$. Each party P_i possess an input x_i. We want to compute a function

$$\begin{gathered} f : \mathbb{F}^n \to \mathbb{F}^n \\ (x_1, \ldots, x_n) \to (y_1, \ldots, y_n) \end{gathered}$$

The mapping between input and output is described as an arithmetic circuit.

Definition. An *arithmetic circuit* is a directed, acyclic graph. Each node is called a *gate* and each edge is called a *wire*. There are five types of gates:

- input gates
  - no incoming wires
  - one outgoing wire
- addition and multiplication gates
  - two incoming wires
  - any number of outgoing wires
- multiply by constant gates
  - one incoming wire
  - any number of outgoing wires
- output gates
  - one incoming wire
  - no outgoing wires

2 Game Theory

In this lecture we will discuss games in which players choose their strategy randomly. Therefore it will be necessary to expand our idea of a NE. Forthermore we will introduce an instance that gives a proposition for a strategy to each player and we will examine the effect of such an instant.

2.1 Solutions in mixed strategies

We want that each player choose his strategy with a certain probability. Therefore we need some notation.

Let $\Delta(A_i)$ denote the set of probability distributions on A_i. A *mixed strategy* is juste an element $s_i \in \Delta(A_i)$, in contrast to a pure strategy $a_i \in A_i$. For any $x \in A_i$ we have now

$$s_i(x) = \mathrm{Prob}_{s_i}(a_i = x).$$

The set of all $x \in A_i$ with $s_i(x) > 0$ is called the support of s_i. We write

$$\mathrm{supp}(s_i) = \{x \in A_i | s_i(x) > 0\}.$$

We will assume *risk-neutrality*. What it means we see in the following example.

Example. We consider the game *who will be the millionaire*. A person has reached 25,000$. Now he can stop the game and will get 25,000$ for sure or he can guess the answer of the next question. If he choose the right one he wins 100,000$, otherwise only 10,000$. What should he do?

In order to answer this question we compute the expected value. The person can expect a gain of $1/4 \cdot 100,000 + 3/4 \cdot 10,000$\$ which is more than 25,000$. What we mean with *risk-neutrality* is that the person will decide to guess the answer cause of the higher expected value even if there is a (high) probability to loose an amount of money.

So we need to compute expected utlities by linear combinations. We write

$$u_i(s) = \mathrm{E}_{x \in A}(u_i(s(x))).$$

With this notation we can give an expanded definition of a NE.

Definition. A vector $s = (s_1, \ldots, s_n)$ of mixed strategies in a game $G = (N, (A_i), (u_i))$ is a *mixed Nash Equilibrium*, if for each player i and every mixed strategy $s_i' \in \Delta(A_i)$, we have

$$u_i(s_i, s_{-i}) \geq u_i(s_i', s_{-i}).$$

Example (BoS). We consider the game Baseball or Softball given by the following table:

	B	S
B	$(2,1)$	$(0,0)$
S	$(0,0)$	$(1,2)$

We claim that $s = (\underbrace{(2/3, 1/3)}_{=s_1}, \underbrace{(1/3, 2/3)}_{=s_2})$ is a mixed NE. The expected utility of player 1 is $u_1 = \frac{2}{9} \cdot 2 + \frac{2}{9} \cdot 1 = \frac{2}{3}$. We consider the case where player 1 changes his strategy s_1 to $s_1' = (p, 1-p)$. Then the expected utility is

$$u_1(s') = 2p \cdot \frac{1}{3} + (1-p) \cdot \frac{2}{3} \cdot 1 = \frac{2p}{3} + \frac{2}{3} - \frac{2p}{3} = \frac{2}{3}.$$

We saw that the utility doesn't change if player 1 changes his strategy. The same argument works also for player 2 as the utlily functions are symmetric. Hence s is a mixed NE.

Theorem (Nash, 1951)**.** *Every finite strategy game has a mixed NE.*

Proof idea. One can proof the theorem by defining a best-response function $B : A \to \{A\}$ (:= power-set of A), extend to $\Delta A_1 \times \ldots \times \Delta A_n \to \{\Delta A_1 \times \ldots \times \Delta A_n\}$. One observe that s is a mixed NE iff $s \in B(s)$. This leads to a fixpoint theorem. □

2.2 Correlated equilibria

Now we want to introduce a third instance that gives propositions to the players.

Definition. A *mediated version* of the game G consists of two steps:

1. A *mediator* chooses a vector of actions $a = (a_1, \cdots, a_n)$ according to some distribution M. She hands a_i (as recommendation) to player i.
2. The players play G.

Definition. A distribution $M \in \Delta(A)$ is a *correlated equilibrium* if for all $a \in \mathrm{supp}(M)$, for all $i \in N$ and for all $a_i' \in A_i$, the following holds:

$$u_i(a_i', a_{-i}|a_i) \leq u_i(a_i, a_{-i}|a_i).$$

Example. We look at the game given by the following table:

	L	M	R
U	$(2,1)$	$(1,2)$	$(0,0)$
M	$(0,0)$	$(2,1)$	$(1,2)$
D	$(1,2)$	$(0,0)$	$(2,1)$

There are

no pure NE

one mixed NE $\left(\frac{1}{3},\frac{1}{3},\frac{1}{3}\right)\left(\frac{1}{3},\frac{1}{3},\frac{1}{3}\right)$ with expected payoff 1.

at least one correlated equilibrium by

$$M \in_{\mathrm{R}} \{(U,L),(U,M),(M,M),(M,R),(D,L),(D,R)\}$$

uniformly for an expected payoff of $\frac{3}{2}$.

3 Exercises

3.1 Exercise 1.2

(i) $f(x_1,x_2,x_3) = (x_1 =^? x_2)\cdot(x_2 =^? x_3)$.

(ii) $a =^? b$ corresponds to $1-(a-b)^{p-1} \mod p$.

(iii) $(x_1-x_2)^2+(x_2-x_3)^2+(x_1-x_3)^2 =^? 0 \mod p$ where $p \geq 3g^2+1$

3.2 Exercise 1.3

Actually the exercise is wrong. If the value of the offered object is 0, then the dominant strategy is to bid 0. So let's assume that the object has a positive value.

If we win the auction (with a positive bid), we could have bidden less than our actual bid because the other bids are lower. So we have found a situation where the strategy to bid a positive value is not optimal and hence not dominant.

So let's see what happen if we don't bid. Then we could loose the auction even if all players also bid 0. Then we could have won with a very small bid and we could have gained a almost the value of the offered object.

We see to give a bid or not is in some situations not optimal. Hence there is no dominant strategy.

3.3 Exercise 1.4

If $G=(N,A,(u_i))$, then the strategic game is

$N = \{P_1,P_2\}$

$A = \mathbb{R}_0^+$

$$u_1(t_1,t_2) = \begin{cases} -t_1 & t_1 < t_2 \\ v_1/2 - t_1 & t_1 = t_2 \\ v_1 - t_2 & t_1 > t_2 \end{cases}$$

In a pure NE the situation that $t_1 = t_2$ never occurs. So one of the players can increase his gain to 0 conceding immediately.