


Secure Computation: Part II
Prof. Ashish Choudhury
Department of Computer Science and Engineering
Indian Institute of Science, Bengaluru

Lecture - 21
Properties of Polynomial Over a Field: I

(Refer Slide Time: 00:29)


Lecture Overview



- Polynomials over fields
 - ❖ Properties
 - ❖ Lagrange's interpolation

(Refer Slide Time: 00:34)

Polynomials Over a Field



□ Let $(\mathbb{F}, +, \cdot)$ be a field

□ **Definition:** a **t -degree polynomial** $f(X)$ over \mathbb{F} is of the form

$$f(X) = a_0 + a_1 \cdot X + \dots + a_t \cdot X^t$$

All operations are field operations

$\left. \begin{array}{l} a_0, \dots, a_t \in \mathbb{F} \\ \text{+1 Coefficients} \end{array} \right\}$
 $\mathbb{F} = \{0, 1, 2, 3, 4, 5, 6\}$

□ Ex: consider the field $(\mathbb{Z}_7, +_7, \cdot_7)$ --- addition/multiplication modulo 7

$$f(X) = \underline{6} + \underline{2}X + \underline{3}X^4 \quad \underline{8} = 8 \bmod 7 = 1$$

$$f(1) = (\underline{6} + \underline{2} + \underline{3}) \bmod 7 = 4$$

$$f(\underline{8}) = f(\underline{1}) = (\underline{6} + \underline{2} + \underline{3}) \bmod 7 = \underline{4}$$

additive identity element

□ **Definition (root of a polynomial):** an element $v \in \mathbb{F}$ is called a **root** of $f(X)$, if $f(v) = 0$

one root $\left\{ \begin{array}{l} f(X) = 6 + 2X + 3X^4 \\ f(0), f(1), \dots, f(5) \neq 0 \end{array} \right.$	$\left. \begin{array}{l} X=6 \\ g(X) = X + 4X^2 + X^3 + X^4 \\ g(\underline{0}) = g(\underline{1}) = g(\underline{2}) = g(\underline{3}) = 0 \end{array} \right\} 4 \text{ roots}$
--	--

Hello everyone. Welcome to this lecture. So, in this lecture we will discuss about polynomials over Fields and Lagrange interpolation. So, what are polynomials over fields?

Imagine you are given a field \mathbb{F} with the abstract $+$ and \cdot operations, then a t -degree polynomial over this field will have the form as follows. So, it will have $t + 1$ coefficients and all this $+$ and \cdot operations are the $+$ and \cdot operations of your finite field.

Now, well the field need not be finite, it could be an infinite field. So, all this $+$ and \cdot operations are the field operations. So, for instance if we consider the field \mathbb{Z}_7 where the operations are addition modulo 7 and multiplication modulo 7. Then, consider this polynomial $f(X)$, where the coefficients are 6, 2 and 3. So, \mathbb{Z}_7 will have the elements 0, 1, 2, 3, 4, 5 and 6.

Then, if you want to find out the value of the polynomial at $X = 1$, then $f(1)$ will be $6 + 2 + 3$. And, since all the summation and multiplication operations, all the addition and the multiplication operations are then modulo 7, the result will be 4. If we want to compute the value of this polynomial at $X = 8$, then there are two ways to do that. Either we can substitute the value of $X = 8$, solve and finally, do mod 7 that will give us the answer.

But what we can do is that the element 8 in this field will be same as the element 1, because 8 will be same as 8 modulo 7 in this field which will be the element 1. So, the value of the polynomial at $X = 8$ will be the same as the value of the polynomial at $X = 1$. And, we have already calculated the value of the polynomial at $X = 1$. Next, we want to define the root of a polynomial over the field.

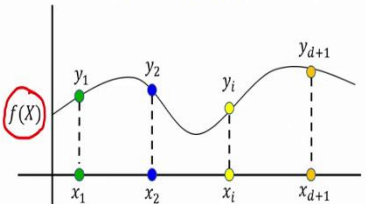
So, an element v from the field is called the root of the polynomial if the value of the polynomial at that element v or $X = v$ turns out to be the additive identity element. So, this 0 is the additive identity element. So, for instance if we take again the same polynomial $f(X)$, then it has only one root namely the value $X = 6$. Whereas, if we take this polynomial $g(X)$, then it has 4 roots namely $X = 0, X = 1, X = 2$ and $X = 3$. All turn out to be the root.

(Refer Slide Time: 03:50)

Lagrange's Polynomial Interpolation

← $d+1$ distinct points →

□ **Theorem:** Let $(x_1, y_1), \dots, (x_{d+1}, y_{d+1})$ be pairs of elements from \mathbb{F} , where x_1, \dots, x_{d+1} are distinct. Then there exists a unique d -degree polynomial $f(X)$ over \mathbb{F} , such that $f(x_i) = y_i$, for $1 \leq i \leq d+1$



$d+1$ or more distinct points on a 2-D plane \Rightarrow there is a unique d -deg poly

□ **Idea:** Express the unknown $f(X)$ as a linear combination of $d+1$ d -degree polynomials $\delta_1(X), \dots, \delta_{d+1}(X)$

$$f(X) \equiv y_1 \cdot \delta_1(X) + \dots + y_i \cdot \delta_i(X) + \dots + y_{d+1} \cdot \delta_{d+1}(X)$$

The next thing that we want to discuss is the Lagrange's polynomial interpolation. So, before going through the statement, we know that if we are given $d + 1$ or more distinct points in a 2-dimensional plane, on a 2-dimensional plane; then there is a unique d degree polynomial passing through them, passing through all the $d + 1$ points. But, if you are given d or lesser number of distinct point, then we cannot find a unique polynomial passing through all the given points.

But if $d + 1$ or more distinct points are given, then we can always compute a unique d degree polynomial passing through those given points. So, the Lagrange polynomial interpolation extends that result for the case when your polynomial is over a field. So, the statement of the theorem is as follows. You are given $d + 1$ distinct points. Why they are distinct? Because, the X components of these points are distinct. Then, the statement says that there exists a unique polynomial $f(X)$ whose degree is d and which passes through this given $d + 1$ points.

And the idea behind the proof of this theorem is that, given such $d + 1$ distinct points we can compute the unknown d degree $f(X)$ polynomial. To compute that unknown polynomial, the idea is to express that unknown polynomial as a linear combination of some d degree polynomials. Specifically, $d + 1$ number of d degree polynomials using the combiners $y_1, y_2, \dots, y_i, \dots, y_{d+1}$.

(Refer Slide Time: 06:24)

Lagrange's Polynomial Interpolation

← d+1 distinct points →

Theorem: Let $(x_1, y_1), \dots, (x_{d+1}, y_{d+1})$ be pairs of elements from \mathbb{F} , where (x_1, \dots, x_{d+1}) are distinct. Then there exists a unique d-degree polynomial $f(X)$ over \mathbb{F} , such that $f(x_i) = y_i$, for $1 \leq i \leq d+1$

(X xi)

$$\delta_i(X) = \frac{(X - x_1) \cdots (X - x_{i-1})(X - x_{i+1}) \cdots (X - x_{d+1})}{(x_i - x_1) \cdots (x_i - x_{i-1})(x_i - x_{i+1}) \cdots (x_i - x_{d+1})}$$

$\delta_i(X)$ **polynomial**

Idea: Express the unknown $f(X)$ as a linear combination of d + 1 d-degree polynomials $\delta_1(X), \dots, \delta_{d+1}(X)$

Every xi except xi is the root of $\delta_i(X)$

$$f(X) \equiv y_1 \cdot \delta_1(X) + \dots + y_i \cdot \delta_i(X) + \dots + y_{d+1} \cdot \delta_{d+1}(X)$$

f(xi) = 0 + 0 + ... + yi + 0 + ... = yi

$$\delta_i(x_i) = 1$$

$$\delta_i(x_1) = \dots = \delta_i(x_{i-1}) = \delta_i(x_{i+1}) = \dots = \delta_i(x_{d+1}) = 0$$

$$\delta_{d+1}(x_1) = \dots = \delta_{d+1}(x_d) = 0$$

$$\delta_{d+1}(x_{d+1}) = 1$$

Now, what are these d degree polynomials $\delta_1, \delta_2, \dots, \delta_{d+1}$? Well, if we take the first polynomial $\delta_1(X)$, then the value of that polynomial at x_1 will be 1. And the value of that polynomial at the remaining x values will be 0. So, basically every x_i except x_1 is the root of $\delta_1(X)$ polynomial.

In the same way, if I consider the i th δ polynomial, namely δ_i . Then, all the x values among these $d + 1$ x values except the value x_i will be the root of that polynomial. And, like that if I consider the $d + 1$ th delta polynomial, then all the x values in this set $\{x_1, \dots, x_{d+1}\}$ will be the root of this polynomial except x_{d+1} . At x_{d+1} the value of the polynomial should be 1. So, for the moment assume we have such polynomials $\delta_1, \delta_2, \dots, \delta_{d+1}$.

Then, it is easy to see that our unknown $f(X)$ polynomial will be this, because indeed if we have this system of polynomials $\delta_1, \delta_2, \dots, \delta_{d+1}$. And, then if I evaluate this polynomial at $X = x_i$, then δ_1 evaluated at x_i will turn out to be 0, δ_2 evaluated at x_i will turn out to be 0. So, we will have $0 + 0 + 0 + 0$, but when we go to this i th term. Then, δ_i polynomial evaluated at x_i will be 1 and 1 multiplied with y_i will be y_i , because 1 is the multiplicative identity element.

And then again, all the remaining other terms will be 0, 0, 0 and hence $f(x_i)$ is indeed y_i . And it is easy to see that the degree of $f(X)$ is d , because it is a summation of several d degree polynomials. So, now, the question is what will be the form of the δ_i polynomial?

So, if we want the δ_i polynomial to have these two properties, namely the value of that polynomial should be 1 at $X = x_i$. And all other X values in the set $\{x_1 \text{ to } x_{d+1}\}$, except x_i should be the root then this should be the δ_i polynomial.

So, you can see x_1 is the root, x_2 is the root, x_{i-1} is the root, x_{i+1} is the root, x_{d+1} is a root. The only term which is missing in the numerator is $X - x_i$, that is not there.

(Refer Slide Time: 09:34)

Properties of t -degree Polynomial

□ Let $\mathcal{P}^{s,t}$ be set of all t -degree polynomials over \mathbb{F} , with s as the constant term

✧ Each $f(X) \in \mathcal{P}^{s,t}$ is of the form $f(X) = s + a_1 \cdot X + \dots + a_t \cdot X^t$, where each $a_1, \dots, a_t \in \mathbb{F}$

$|\mathcal{P}^{s,t}| = |\mathbb{F}|^t$ $a_1 - \text{we have } |\mathbb{F}| \text{ options}$
 $a_2 - \text{ " " " } |\mathbb{F}|$

□ Ex: $t = 2$, $\mathbb{F} = (\mathbb{Z}_3, +_3, \cdot_3)$ and $s = 1$ $\mathbb{Z}_3 = \{0, 1, 2\}$

1	1 + X	1 + X ²	1 + X + X ²	1 + 2X + X ²
1 + 2X	1 + 2X ²	1 + X + 2X ²	1 + 2X + 2X ²	

$1 + 0 \cdot X + 0 \cdot X^2$ $\mathcal{P}^{1,2}$

□ $\{(x_{i_1}, y_{i_1}), \dots, (x_{i_t}, y_{i_t})\} \dots$ arbitrary values from \mathbb{F} :

$x_{i_1} \neq \dots \neq x_{i_t} \neq 0$

Now, let us see some more properties of t -degree polynomials which will be useful for us. So, let me denote the set of all t -degree polynomials over a field with s being the constant term by this notation $\mathcal{P}^{s,t}$. And any polynomial in this set will consist of $t + 1$ coefficients, where the constant term or the coefficient for the constant term is fixed. It is s .

But a_1 could be any element from the field, a_2 could be any element from the field and a_t could be any element from the field. So, it is easy to see that the number of such polynomials is nothing but $|\mathbb{F}|^t$, because for a_1 we have $|\mathbb{F}|$ number of options. Because we could have these many candidate a_1 coefficients and independent of a_1 , the number of candidate a_2 coefficients also is $|\mathbb{F}|$ and so on.

So, if you want to see an example, take this field \mathbb{F} . And suppose t is equal to 2 and s is equal to 1. So, what will be the set of all possible 2-degree polynomials whose constant term is 1? Well, that set is this. So, this constant term 1 can be treated as a 2 degree

polynomial, because I can treat this polynomial as the constant term being 1. Then, the coefficient of X is 0 and the coefficient of X^2 is 0.

In the same way, the polynomial $1 + X^2$ can be interpreted as a polynomial, where the coefficient of X is 0 and the coefficient of X^2 is 1 and so on. And the constant term is fixed. So, you see the constant term is fixed to 1 and the degree does not go beyond 2. So, this will be the collection of polynomials and all the coefficients are from the set \mathbb{Z}_3 which will have the element 0, 1 and 2. Now, the next result is the following which is again a very standard result.

(Refer Slide Time: 12:13)

Properties of t -degree Polynomial

□ Let $\mathcal{P}^{s,t}$ be set of all t -degree polynomials over \mathbb{F} , with s as the constant term

❖ Each $f(X) \in \mathcal{P}^{s,t}$ is of the form $f(X) = s + a_1 \cdot X + \dots + a_t \cdot X^t$, where each $a_1, \dots, a_t \in \mathbb{F}$
 $|\mathcal{P}^{s,t}| = |\mathbb{F}|^t$ a₁ - we have |F| options
a₂ - " " |F|

□ Ex: $t = 2$, $\mathbb{F} = (\mathbb{Z}_3, +_3, \cdot_3)$ and $s = 1$ 4 + 0 · X + 1 · X² Z₃ = {0, 1, 2}

1	1 + X	1 + X ²	1 + X + X ²	1 + 2X + X ²
1 + 2X	1 + 2X ²	1 + X + 2X ²	1 + 2X + 2X ²	

→ t arbitrary distinct points

□ $\{(x_{i_1}, y_{i_1}), \dots, (x_{i_t}, y_{i_t})\}$ arbitrary values from \mathbb{F} :
 $x_{i_1} \neq \dots \neq x_{i_t} \neq 0$ together (++)

□ For any given $s \in \mathbb{F}$, there is a unique polynomial from $\mathcal{P}^{s,t}$ passing through $\{(0, s), (x_{i_1}, y_{i_1}), \dots, (x_{i_t}, y_{i_t})\}$

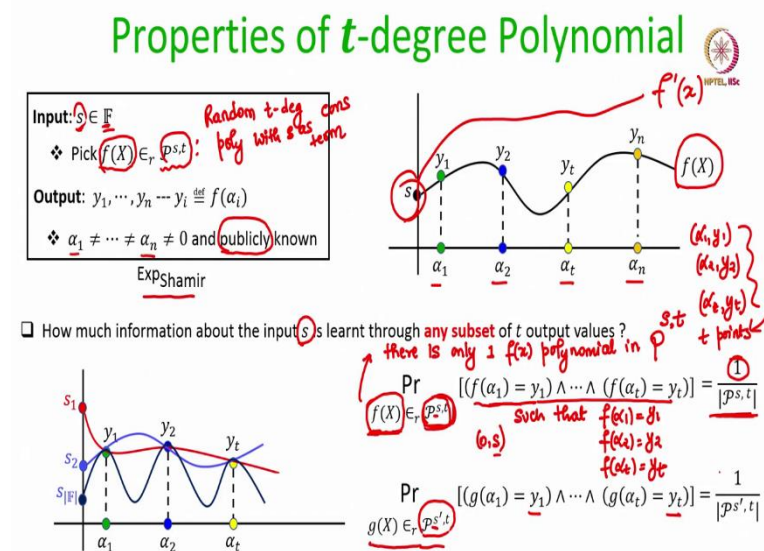
So, if we take a 2-dimensional plane and if I give you one point on the straight line. And now, if I ask you how many straight lines can I have passing through this circle point whose constant term is s ? There is only one straight line. If I ask you how many straight lines can I have passing through the circle point whose constant term is s' ? Again, there is only one straight line. If I ask you how many straight lines can I have passing through this circle point whose constant term is s'' ? Again, there is only one straight line.

So, we can extend that result for the case of finite field for any degree polynomial. So, imagine you are given t distinct points, t arbitrary distinct points. Why they are distinct? Because, the X components are all distinct and all of all the X components are non-zero. Then, the claim is that you take any value from the field, there is only a single t -degree polynomial whose constant term will be s and which passes through the given t points.

So, pictorially I am fixing the t points, where all the t points are distinct. And now, I am asking how many polynomials of degree t can be there whose constant term is s and which passes through these t points? Well, there can be only one such polynomial, because that polynomial must pass through $(0, s)$ as well. Namely, the point $(0, s)$ lies on that polynomial and anyhow I am giving you t more points also to lie on that polynomial.

So, all together, we have $t + 1$ points and through $t + 1$ points, we can have only one t -degree polynomial passing. In the same way, if I ask you how many polynomials can be there whose degree is t , whose constant term is, say s' , and which passes through these given t points? The answer is there is only one such polynomial, say $g(X)$.

(Refer Slide Time: 14:48)



Now, based on these properties of t -degree polynomials, let us see an experiment which is a randomized experiment. It is a randomized experiment, in the sense that even if the input of the experiment is same, the output could be different with different probabilities. So, the input is a value from the field. Now, to generate the output the experiment picks a random t -degree polynomial.

So, a random t -degree polynomial with s as constant term and then to generate the output, it evaluates that polynomial at n publicly known distinct points. So, f is computed at α_1 , f is computed at α_2 , f is computed at α_n , where all these α components are distinct, different from 0 and that is the output for this experiment.

So, we can see why this is a randomized experiment. If I run this experiment 2 times, again if I run it 2 times with the same input s . Then, the outputs y_1, \dots, y_n will be different with different probabilities because, the outputs are the points on the polynomial which is selected here randomly.

So, the probability that the polynomial turns out to be the same during both the invocations of this experiment is small. It is of course, non-zero, but it is small; assuming that your field is sufficiently large. So, pictorially the output of the experiment is select determined as follows. The input is fixed, to generate the output a random curve is picked whose constant term is s and the value of that and n points on that curve are given as the output.

Again, if you want to run the experiment with input s , next time probably you would have chosen the polynomial $f'(X)$ and then the outputs would have been different. The α components remain the same throughout the experiment. So, the components does not change, it is fixed once for all and it will be publicly known. Now, we want to analyze here that how much information about the input s is learnt through any subset of t output values?

So, what I am asking here is the following. Suppose you can see only t output values in this experiment. You do not know the value of s , but you know the steps of the experiment. You know that I would have picked a random polynomial whose degree would have been t and whose constant term would have been my input. And I would have given you t output values, because you can see only t output values, not the full vector of n values.

Now, the question is how much information about my input you learn in this experiment? So, pictorially I am asking you the following question. So, imagine that you observe the first t output values. Now, based on those t output values and anyhow the components $\alpha_1 \dots, \alpha_t$ are also known to you; can you tell whether my input was s_1 or my input was s_2 or whether my input was any other value from the field? The claim is the following.

With equal probability the t output values could result for the input being s as well as the input being s' . More specifically, if we consider an instance of this experiment where the input would have been s . And, if we consider another instance of the same experiment where input would have been s' , then with equal probability you would have seen the values $y_1 \dots y_t$ as the first t output values that is the claim here.

So, formally if we take the probability over all possible t -degree polynomials $f(X)$ which are randomly selected from this set. The probability that the randomly chosen polynomial from this set evaluates to y_1, y_2, \dots, y_t at $\alpha_1, \alpha_2, \dots, \alpha_t$ is equal to 1 over the size of the number of t -degree polynomials with s being the constant term.

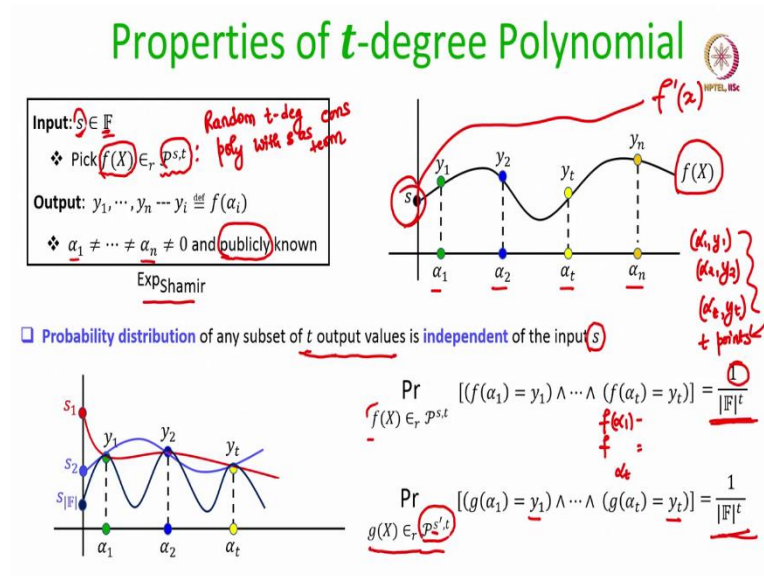
This is because when we are taking the probability over all candidate $f(X)$ polynomial, there is only 1 $f(X)$ polynomial in this bigger set of all t -degree polynomials with s being the constant term, such that polynomial evaluated at α_1 would have given you y_1 , that polynomial evaluated at α_2 would have given you y_2 . And, that polynomial evaluated at α_t would have given you y_t .

This is because $(\alpha_1, y_1), (\alpha_2, y_2), \dots, (\alpha_t, y_t)$; it constitutes t points and that point though those t points along with 0, s determines a unique t -degree polynomial. So, among all possible polynomials from this set of polynomials there is exactly 1 $f(X)$ polynomial which satisfies this condition. For all other $f(X)$ polynomials in this set the condition will not be satisfied.

Now, what is the probability that in this experiment indeed that specific polynomial $f(X)$ is selected here? Remember, the polynomial from the set is picked randomly. So, among all the polynomials with degree t and s being the constant term, the probability that experiment would have selected that special polynomial $f(X)$ whose constant term is s and which evaluates to y_1, \dots, y_t at $\alpha_1, \dots, \alpha_t$ is 1 over the sample space.

The sample space is the set of all such polynomials and the favorable element or the favorable number of polynomials is only 1 polynomial. And, now due to the same reason we can argue that if we now take the probability over the set of all t -degree polynomials selected randomly, whose constant term being s' . The probability that any such randomly chosen polynomial would have evaluated to y_1, y_2, \dots, y_t is also the same as 1 over the number of t -degree polynomials with s' being the constant term.

(Refer Slide Time: 22:54)



But if you see closely, the number of t -degree polynomials with s being the constant term and the number of t -degree polynomials with s' being the constant term is same. Namely, $\frac{1}{|\mathbb{F}|^t}$. So, that shows the following that if there is an observer who observes or who learns the output of this experiment, it learns only a subset of t output values, instead of all n output values.

Then, from the viewpoint of that observer, the probability distribution of those t output values it does not depend on s . Those t output values could occur as the output of the experiment for s ; with the same probability with which those output values would have occurred as the output, if s' would have been the input of the experiment.

(Refer Slide Time: 23:58)

Properties of t -degree Polynomial

Input: $s \in \mathbb{F}$ S: Secret

❖ Pick $f(X) \in_r \mathcal{P}^{s,t}$ 17

Output: $y_1, \dots, y_n \dots y_i \triangleq f(\alpha_i)$

❖ $\alpha_1 \neq \dots \neq \alpha_n \neq 0$ and publicly known

Ex: $n = 5, t = 2, \mathbb{F} = (\mathbb{Z}_{17}, +_{17}, \cdot_{17})$ and $s = 13$

$\alpha_1 = 1, \alpha_2 = 2, \alpha_3 = 3, \alpha_4 = 4, \alpha_5 = 5$ 2 17

$f(X) = 13 + 10X + 2X^2$

$y_1 = 8 \quad y_2 = 7 \quad y_3 = 10 \quad y_4 = 0 \quad y_5 = 11$

Can $y_1 = 8$ and $y_3 = 10$ occur as the output for every candidate $s \in \mathbb{Z}_{17}$, apart from $s = 13$?

Candidate s	Candidate $f(X)$	y_1	y_3
0	$16X + 9X^2$	8	10
1	$1 + 9X + 15X^2$	8	10
2	$2 + 2X + 4X^2$	8	10
3	$3 + 12X + 10X^2$	8	10
4	$4 + 5X + 16X^2$	8	10
5	$5 + 15X + 5X^2$	8	10
6	$6 + 8X + 11X^2$	8	10
7	$7 + X$	8	10
8	$8 + 11X + 6X^2$	8	10
9	$9 + 4X + 12X^2$	8	10
10	$10 + 14X + X^2$	8	10
11	$11 + 7X + 7X^2$	8	10
12	$12 + 13X^2$	8	10
13	$13 + 10X + 2X^2$	8	10
14	$14 + 3X + 8X^2$	8	10
15	$15 + 13X + 14X^2$	8	10
16	$16 + 6X + 3X^2$	8	10

So, let me demonstrate this with an example to make it clearer. So, let us take specific values for n, t and the concrete field and the concrete value of the candidate secret or candidate s . The s here is called as the secret. So, imagine the value of s is 13; that means, someone runs this experiment with the input 13.

Now, there are many polynomials of degree 2 with 13 being the constant term. Specifically, there are 17 square number of such polynomials. Among all such polynomials, one such polynomial is picked randomly in the experiment. So, suppose we also fix the evaluation points $\alpha_1, \alpha_2, \alpha_3, \alpha_4, \alpha_5$ to 1, 2, 3, 4 and 5 respectively. As I said that the polynomial $f(X)$ is picked randomly, suppose in the experiment this polynomial is selected.

The probability that this polynomial is selected is $\frac{1}{17^2}$, because as I said there are 17^2 candidate polynomials. So, the probability that this polynomial is selected is $\frac{1}{17^2}$. Now, if the experiment would have selected this polynomial, then the output would have been the out value of this polynomial at $X = 1, X = 2, X = 3, X = 4, X = 5$.

Now, suppose I do not give you the 5 output values, but I give you only 2 output values say and those 2 output values could be depending upon your choice. You just ask me 2 output values. So, suppose you asked for the first and the third output value. So, I gave you y_1 equal to 8 and y_3 equal to 10. And now I ask you can you tell me what was my

input? My input was 13. Can you tell me what was my input? I will now show you that the following hold. From your view point you know that my input is an element from this field \mathbb{Z}_{17} .

That means, from your viewpoint the candidate s could be 0, it could be 1, it could be 2 or it could be an element 16 as well. And I am challenging you to tell me what my input was, given that you have seen the output values y_1 equal to 8 and y_3 equal to 10. And of course, you know all the alphas, you know the steps of my experiment as well.

I will show that for every candidate value of y , every candidate value of s , and as I have said that there are 17 candidate values of s , you cannot rule out any of them. With equal probability it could be the case that I have run the experiment with input 0. And, if I would have run the experiment with input 0, I could have produced outputs y_1 equal to 8 and y_3 equal to 10 and given to you.

And, with the same probability it could be it will be the case that, I could have run my experiment with input 1 and produced the outputs y_1 equal to 8 and y_3 equal to 10. And, like that with the same probability, it will be the case that I could have run the experiment with input 16 and produce the outputs y_1 equal to 8 and y_3 equal to 10. So, let us see.

So, now this computation you are doing in your mind, because your goal is to find out what exactly was my input. So, you think your mind, you are doing this mental calculation; is it possible that professor's input is 0? Well, there is a probability that professor's input is 0, provided he would have selected the polynomial $16X + 9X^2$.

Because, indeed this candidate polynomial when evaluated at α_1 would have given 8 and when evaluated at α_3 would have given 10 which matches with the output values that the professor has given you. So, you cannot rule out the candidate 0 from your viewpoint.

Now, you are asking the following question: is it possible that professor has run the experiment with input 1? And, the answer is yes, it is quite possible that the professor has run the experiment with input 1; provided he has selected this polynomial. That means, if professor input would have been 1 and if he would have selected this polynomial. And, then if you would have evaluated this polynomial at α_1 and α_3 , you would have seen the outputs 8 and 10.

And, like that there is a possibility that the professor has run the experiment with input 2, where his polynomial was this value. And this polynomial evaluated at α_1 and α_3 would have given the outputs 8 and t as you have observed. And, now like this I can complete the table and then you can see what is happening here is, this is the computation which you have done.

And you cannot rule out any value, any candidate value of s . You have seen outputs 8 and 10. You do not know the polynomial that I have selected. You do not know my input and now you have done a mental calculation. And, as per your mental calculation every candidate s could have resulted in an output y_1 equal to 8 and y_3 equal to 10 in this experiment.

And that is why just seeing the 2 values namely y_1 equal to 8 and y_3 equal to 10 is incomplete for you, is insufficient for you to determine what exactly was my input in this experiment. So, this is a very nice property which we will utilize later on heavily in the course. So, with that I end this lecture.

Thank you.