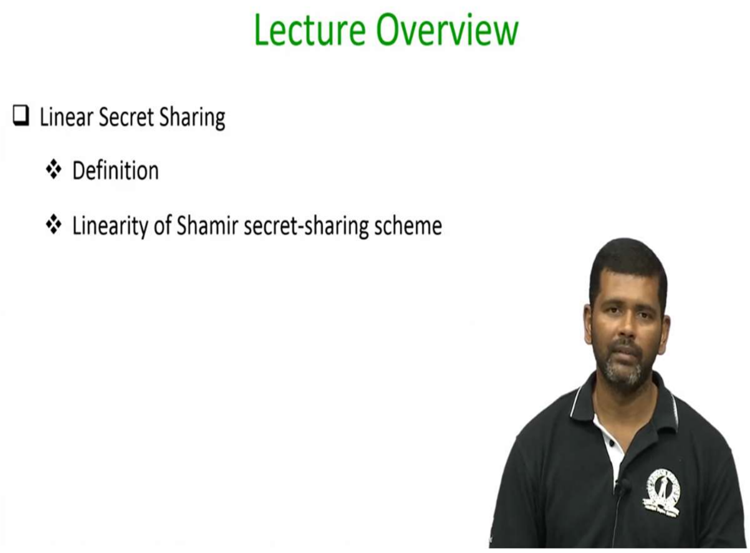
Secure Computation - Part I
Prof. Ashish Choudhury
Department of Computer Science
International Institute of Information Technology, Bangalore

Module - 3
Lecture - 12
Linear Secret-Sharing

(Refer Slide Time: 00:33)

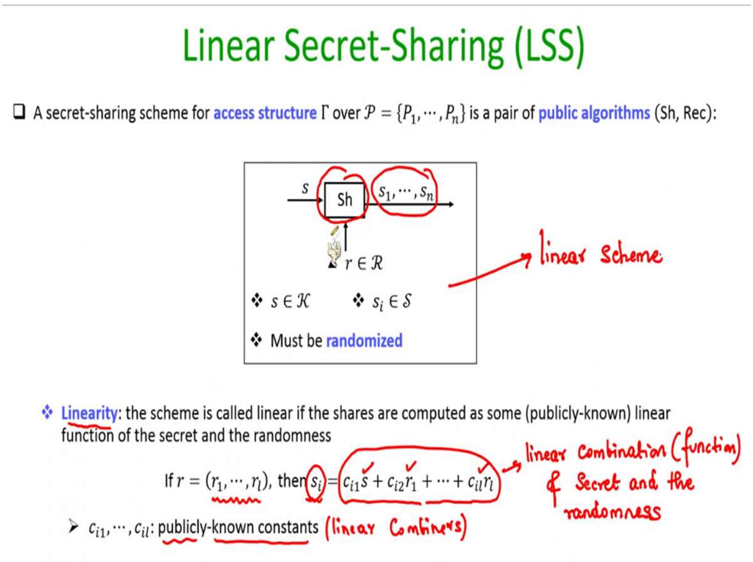


Lecture Overview

- ❑ Linear Secret Sharing
  - ❖ Definition
  - ❖ Linearity of Shamir secret-sharing scheme

Hello everyone. Welcome to this lecture. So, the plan for this lecture is as follows: In this lecture, we will see the definition of linear secret-sharing, which is going to play a very crucial role when we later design MPC protocols. And we will see that our Shamir secret-sharing satisfies the linearity property.

(Refer Slide Time: 00:53)



Linear Secret-Sharing (LSS)

❑ A secret-sharing scheme for access structure Γ over $\mathcal{P} = \{P_1, \cdots, P_n\}$ is a pair of public algorithms (Sh, Rec):

❖ $s \in \mathcal{K}$ ❖ $s_i \in \mathcal{S}$

❖ Must be randomized

❖ Linearity: the scheme is called linear if the shares are computed as some (publicly-known) linear function of the secret and the randomness

If $r = (r_1, \cdots, r_l)$, then $s_i = c_{i1}s + c_{i2}r_1 + \cdots + c_{il}r_l$ linear Combination (function) of Secret and the randomness

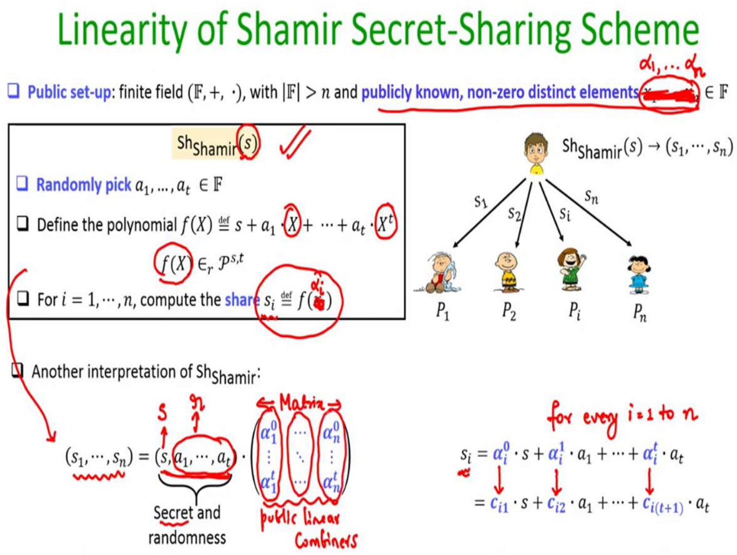
➢ $c_{i1}, \cdots, c_{il}$: publicly-known constants (linear Combiners)

So, linear secret-sharing also known as LSS is as follows: So, recall, our sharing algorithm for a secret-sharing scheme takes a secret s and some internal randomness from the randomness space and generates the shares. So, these shares are computed as some function of your secret under internal randomness. Now, we will say that our secret-sharing algorithm Sh is satisfying the linearity property, or we say that secret-sharing scheme is linear if the shares are computed as some linear function of the secret and the randomness.

What does that mean? It means the following: If my internal randomness is represented by the vector r_1, r_2, r_l, that means, the internal random coins which are generated are r_1, r_2, r_l, during the execution of the sharing protocol. And if it is the case that each share s_i is computed as some linear combination of the secret and the randomness; so, this is a linear combination or a function of secret and the randomness.

And why it is a linear function of secret and the randomness? Because there are this publicly known linear constants which are also called as linear combiners. And your ith share can be expressed as a linear combination of the secret and the components of the randomness. So, if this is the case, then we will say that our sharing algorithm is a linear scheme. That is the definition of linear secret-sharing.

(Refer Slide Time: 03:24)



Linearity of Shamir Secret-Sharing Scheme

❑ Public set-up: finite field $(\mathbb{F}, +, \cdot)$, with $|\mathbb{F}| > n$ and publicly known, non-zero distinct elements $\alpha_1, \ldots \alpha_n$ $\in \mathbb{F}$

$\mathsf{Sh}_{\mathsf{Shamir}}(s)$ ✓

❑ Randomly pick $a_1, \ldots, a_t \in \mathbb{F}$

❑ Define the polynomial $f(X) \overset{\text{def}}{=} s + a_1 \cdot X + \cdots + a_t \cdot X^t$

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

❑ For $i = 1, \cdots, n$, compute the share $s_i \overset{\text{def}}{=} f(\alpha_i)$

$\mathsf{Sh}_{\mathsf{Shamir}}(s) \rightarrow (s_1, \cdots, s_n)$

❑ Another interpretation of $\mathsf{Sh}_{\mathsf{Shamir}}$:

$$(s_1, \cdots, s_n) = \underbrace{(s, a_1, \cdots, a_t)}_{\text{Secret and randomness}} \cdot \underbrace{\begin{pmatrix} \alpha_1^0 & \cdots & \alpha_n^0 \\ \vdots & \ddots & \vdots \\ \alpha_1^t & \cdots & \alpha_n^t \end{pmatrix}}_{\text{public linear Combiners}}$$

for every i = 1 to n

$$s_i = \alpha_i^0 \cdot s + \alpha_i^1 \cdot a_1 + \cdots + \alpha_i^t \cdot a_t$$
$$= c_{i1} \cdot s + c_{i2} \cdot a_1 + \cdots + c_{i(t+1)} \cdot a_t$$

So, now, let us see some instantiations of linear secret-sharing, and we will start with Shamir secret-sharing. So, just to recall, this is the Shamir secret-sharing algorithm, where all the computations are performed over a field. If s is a field element which you want to share as per Shamir secret-sharing, then we randomly pick a polynomial f (X) whose constant term is s and its degree is t, and the shares are the value of this polynomial at n publicly known non-zero distinct field elements x_1 to x_n.

So, now, to see, to verify whether the Shamir secret-sharing satisfies the linearity property, we have to verify whether each share s_i can be expressed as a linear combination of the secret and the randomness. And to verify that, notice that s of i, the share s of i is computed by evaluating the polynomial at X equal to x_i, namely, wherever X is occurring, I have to substitute X equal to x_i, and then only I get the value of s_i.

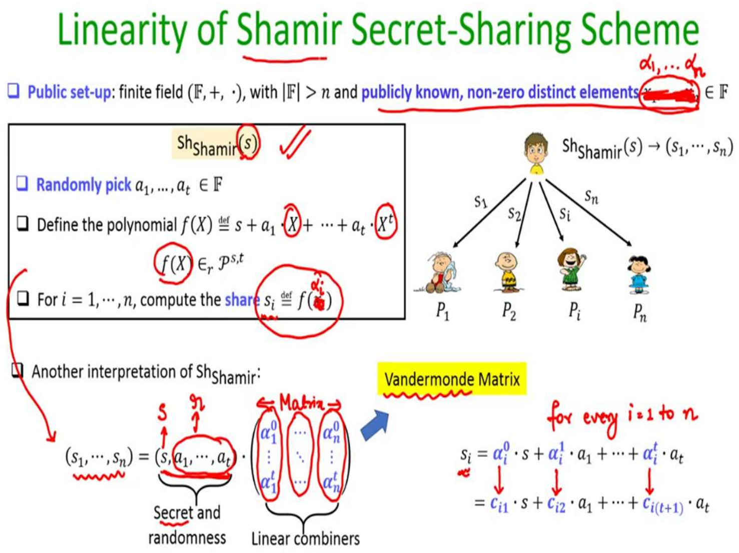
And, okay, so, sorry for the typo here. uh Let me change this publicly known elements as α_1 to α_n, because that is what I am going to use later in my MPC protocols. Right. So, and my share s_i is the value of the f polynomial at X equal to α_i. Right. So, I can keep any n non-zero evaluation points, namely the values at which the shares will be computed. Earlier I called them as x_1 to x_n, but right now, I am calling them as α_1 to α_n; sorry for this typo. Okay. So, my share s of i is computed by substituting X equal to alpha i and if I do that, wherever X is there, I substitute it by alpha i; I get that s of i is this value. Right. So, this holds for every i equal to 1 to n. So, if you want to compute the value of s_i , you have to substitute X equal to α_1; if you want to compute the share s_2, you have to substitute X equal to alpha 2, and so on. And now, this can be interpreted as if my share s_i is a linear function of the secret s and the randomness a_1 to a_t, okay, because I can interpret this $\alpha^0{}_i$ as some constant uh element c_{i1}, from the field; I can interpret this $\alpha^1{}_i$ as c_{i2}; I can interpret this $\alpha^t{}_i$ as some constant $c_{i(t+1)}$.

Right. More specifically, if I consider the vector of Shamir shares which are computed here as per the Shamir secret-sharing, then I can rewrite the vector s_1 to s_n, the share vector, as the following: I can interpret it as the product of this uh row along with this matrix. And the matrix, you have various powers of α_1 to α_n, starting from the 0^{th} power to the t^{th} power. So, now, you can interpret the entire process of uh computing Shamir uh shares as per the Shamir secret-sharing scheme as follows:

So, this vector s along with a_1 to a_t constitute a secret and randomness. Right. So, remember, as per our abstract notation of secret-sharing, there is an internal randomness. That internal randomness is, in Shamir secret-sharing scheme, is this vector of coefficients for the f (X) polynomial. That constitutes your internal randomness. And this is your secret s. And these are my public linear combiners. Okay. And hence, this satisfies the definition of linearity property, right.

So, each share,s_1 is a linear function of your secret randomness and a linear combiners will be the first column of this matrix; s_2 will be considered as a linear combination of your secret randomness and the second column of this matrix. And like that, the n^{th} share will be considered as a linear combination of your secret randomness and the n^{th} column of this matrix. And that is why Shamir secret-sharing scheme satisfies the linearity property. (refer time: 08:49) Okay. So, now, this uh vector, this matrix of linear combiners or ; this matrix has got very nice properties.

(Refer Slide Time: 08:49)



Linearity of Shamir Secret-Sharing Scheme

❑ Public set-up: finite field $(\mathbb{F}, +, \cdot)$, with $|\mathbb{F}| > n$ and publicly known, non-zero distinct elements [redacted] $\in \mathbb{F}$ $\alpha_1, \dots \alpha_n$

$\mathsf{Sh}_{\mathsf{Shamir}}(s)$ ✓

❑ Randomly pick $a_1, \dots, a_t \in \mathbb{F}$

❑ Define the polynomial $f(X) \stackrel{\text{def}}{=} s + a_1 \cdot X + \cdots + a_t \cdot X^t$

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

❑ For $i = 1, \cdots, n$, compute the share $s_i \stackrel{\text{def}}{=} f(\alpha_i)$

$\mathsf{Sh}_{\mathsf{Shamir}}(s) \rightarrow (s_1, \cdots, s_n)$

❑ Another interpretation of $\mathsf{Sh}_{\mathsf{Shamir}}$:

$$(s_1, \cdots, s_n) = \underbrace{(s, a_1, \cdots, a_t)}_{\text{Secret and randomness}} \cdot \underbrace{\begin{pmatrix} \alpha_1^0 & \cdots & \alpha_n^0 \\ \vdots & \ddots & \vdots \\ \alpha_1^t & \cdots & \alpha_n^t \end{pmatrix}}_{\text{Linear combiners}}$$

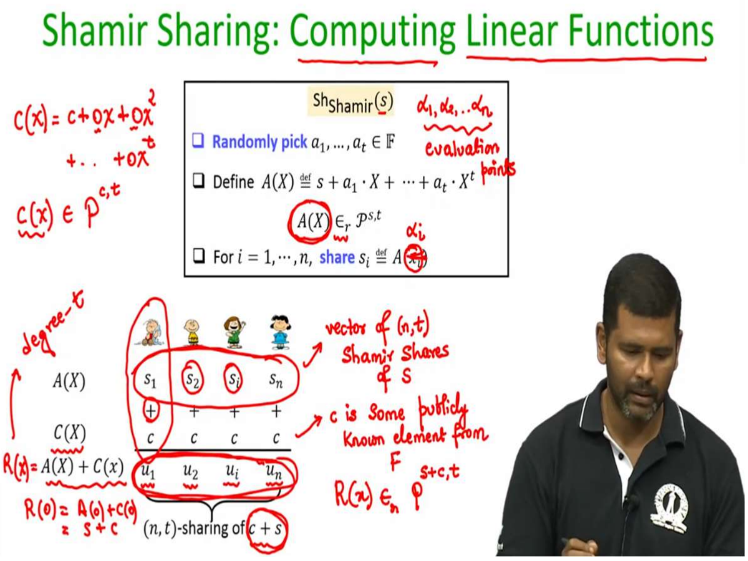
Vandermonde Matrix

for every i = 1 to n

$$s_i = \alpha_i^0 \cdot s + \alpha_i^1 \cdot a_1 + \cdots + \alpha_i^t \cdot a_t$$
$$= c_{i1} \cdot s + c_{i2} \cdot a_1 + \cdots + c_{i(t+1)} \cdot a_t$$

So, now, this matrix of linear combiners, this matrix has got very nice properties. And in linear algebra, we have a special name for this matrix; this matrix is called as Vandermonde matrix. We will come back to the matrix again later and explore some nice properties of this Vandermonde matrix. So, we have shown that Shamir secret-sharing scheme satisfies the linearity property.

(Refer Slide Time: 09:23)



Shamir Sharing: Computing Linear Functions

$\mathsf{Sh}_{\mathsf{Shamir}}(s)$ $\alpha_1, \alpha_2, \dots \alpha_n$ evaluation points

❑ Randomly pick $a_1, \dots, a_t \in \mathbb{F}$

❑ Define $A(X) \stackrel{\text{def}}{=} s + a_1 \cdot X + \cdots + a_t \cdot X^t$

$A(X) \in_r \mathcal{P}^{s,t}$

❑ For $i = 1, \cdots, n$, share $s_i \stackrel{\text{def}}{=} A(\alpha_i)$

$C(x) = c + 0x + 0x^2 + \dots + 0x^t$

$C(x) \in P^{c,t}$

degree-t

$A(X)$	s_1	s_2	s_i	s_n
	+	+	+	+
$C(X)$	c	c	c	c
$R(x) = A(X) + C(x)$	u_1	u_2	u_i	u_n

$R(0) = A(0) + C(0) = s + c$

(n, t)-sharing of $c + s$

vector of (n,t) Shamir Shares of s

c is some publicly known element from F

$R(x) \in_n P^{s+c,t}$

And since Shamir secret-sharing scheme satisfies the linearity property, now we will see some very nice properties; we will see some magic; namely, we will see that how it is possible to compute linear functions of secrets which are shared as per Shamir secret-sharing scheme, without knowing the secrets, but by performing the operations on the shares themselves.

So, imagine that there is some value s which is secret-shared as per Shamir secret-sharing scheme.

So, this is your vector of (n , t) Shamir shares of some value s. So, imagine that the value s is not known to anyone. There was a dealer who has secret-shared value s. Party 1 has the share s_1; party 2 has the share s_2; party i has to share s_i; and party n has the share s_n. Again, uh let us not uh call these evaluation points as x_i, but rather let us call them as α_i.

So, from now onwards, I will assume that all the evaluations are happening at α_1, α_2 and α_n, which are non-zero and distinct and publicly known elements from the field. So, these are our evaluation points. That means, these evaluation points are fixed once for all, and all instances of Shamir secret-sharing scheme will use them as the evaluation points while computing the shares. So, that means, the value s is secret-shared, say by picking a random polynomial A of X, whose degree was t and constant term was s; and that polynomial was evaluated at X equal to α_1 and gave you the share s_1; evaluated at α_2, gave you the share s_2, and so on.

And no one knows the value of secret s; it is some value which is secret-shared. And as a whole, this is now a vector of n shares. I stress that no single party has this full vector; but rather, component wise, each party has the corresponding component of this vector. And now, imagine that c is some publicly known element from s, from your field F. Okay. Everyone knows this; all the n parties knows the value of this (sec) uh public constant, public element, c. It could be any element, 0, 1, any element from the field.

Now, imagine that each party locally adds the s_h respective shares of s. No one knows the value of s, but they have shares of some unknown value s. To their respective shares, each party add the public value c. Okay. This can be done because this is a + operation of your field. So, what I am saying is, P_1 takes the value s_1 and adds the element c. In parallel, P_2 takes the value s_2 and adds the value c. In parallel, the ith party P_i takes the share s_i and adds a value c, and so on.

Now, since the field satisfies the closure property with respect to the + operation, they will obtain; the addition operation will result in another set of field elements. So, let u 1 be the result of P 1's addition; u 2 be the result of second party's addition; u i be the result of ith party's addition; and u n be the result of nth party's addition. Again now, this is a vector of n values.

Now, since the field satisfies the closure property with respect to the + operation, they will obtain; the addition operation will result in another set of field elements. So, let u_1 be the result of uh P 1's addition; u_2 be the result of second party's addition; u_i be the result of i^{th} party's addition; and u_n be the result of nth party's addition. Right. Again now, this is a vector of n values. Now, the question is, is this vector of n values, namely u_1 to u_n are; is is it an arbitrary vector of n field elements or does it constitute some special property?

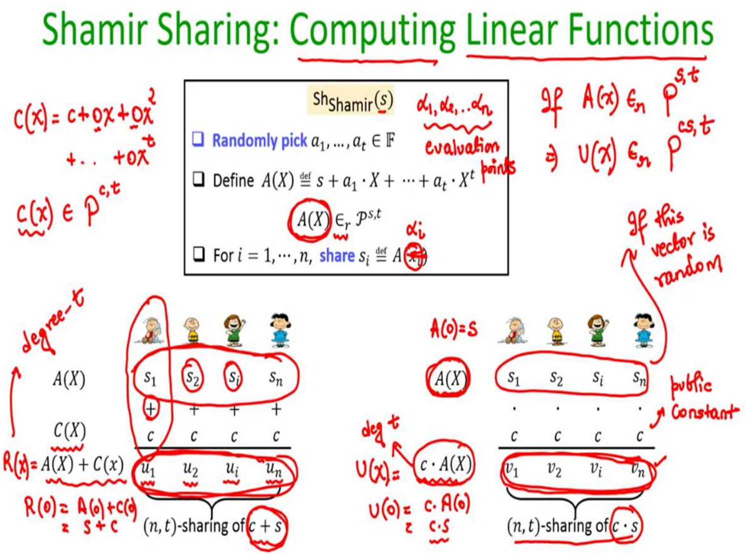
It turns out that it is not an arbitrary vector of n field elements, but rather it has the property that it constitutes a vector of (n , t) Shamir shares of the element c + s. This is because, if I consider a polynomial C(X), which is the constant polynomial; namely, the polynomial c(x) is of the form c; its constant term is c, + all other coefficients are 0; namely, 0 * x, 0 * x^2, and like that, 0 * x^t. So, I can say that c(x) is a polynomial belonging to the set of all possible polynomials whose constant term is this element c and whose degree is t.

I can treat this c(x) as an element of that bigger set of polynomials. It is fine if the remaining coefficients apart from the constant term is 0, but it will be considered as a t-degree polynomial. So, now, if I consider this vector of uh new values u_1 to u_n, I can say that they are values of the polynomial A (X) + C(x), call that polynomial as, say R(X). So, let R of X be the summation of A(X) and C (x) polynomial. And R of X polynomial evaluated at α_1 is basically s_1 + c, which is u_1. R(α_2) is basically u_2; R (α_i) is u_i; and R of α_n is u_n. And what is the degree of R(X)? It is a t-degree polynomial. Right. So, it is a de t-degree polynomial, degree-t. Why? Because A(X) is a t-degree polynomial C(x) is a t-degree polynomial; if you add two t-degree polynomials over a field, you still get a t-degree polynomial. And what can you say about the constant term of R (X)? The constant term of R(X) will be the summation of constant term of A and the constant term of C polynomial.

The constant term of the A polynomial is the value s; the constant term of the C polynomial is c. That means, I can say that R of x is one of the polynomials, okay, from the set of all possible polynomials whose constant term is s + c and whose degree is t. And moreover, if my A (X) polynomial was randomly chosen, I can say that R(X) polynomial is also randomly chosen. That means, this vector of n values u_1 to u_n actually lies on a random t-degree polynomial whose constant term is s + c. I stress here that no party still learns the value of s or the value of s + c; they have just performed the operation individually on their respective shares of s and c, that is all.

And as a result, now they have got a vector of; they have individually got a share of the value c + s, without even knowing the value c, without even knowing the value s; of course, c is publicly known.

(Refer Slide Time: 17:31)



Shamir Sharing: Computing Linear Functions

$\mathsf{Sh}_{\mathsf{Shamir}}(s)$

❑ Randomly pick $a_1, \ldots, a_t \in \mathbb{F}$

❑ Define $A(X) \stackrel{\text{def}}{=} s + a_1 \cdot X + \cdots + a_t \cdot X^t$

$A(X) \in_r \mathcal{P}^{s,t}$

❑ For $i = 1, \cdots, n$, share $s_i \stackrel{\text{def}}{=} A(i)$

$C(x) = c + 0x + 0x^2 + \ldots + 0x^t$
$C(x) \in \mathcal{P}^{c,t}$
$\alpha_1, \alpha_2, \ldots \alpha_n$
evaluation points
α_i
If $A(x) \in_r \mathcal{P}^{s,t}$
$\Rightarrow U(x) \in_r \mathcal{P}^{cs,t}$
If this vector is random
degree-t
$A(X)$
s_1 s_2 s_i s_n
$C(X)$
c c c c
$R(x) = A(X) + C(x)$
u_1 u_2 u_i u_n
$R(0) = A(0) + C(0) = s + c$
(n,t)-sharing of $c + s$
$A(0) = s$
$A(X)$
public Constant
deg t
$U(x) = c \cdot A(X)$
v_1 v_2 v_i v_n
$U(0) = c \cdot A(0) = c \cdot s$
(n,t)-sharing of $c \cdot s$

In the same way, imagine I take another operation where parties have a share, parties have their respective shares of some unknown value s, s_1 to s_n; and suppose they lie on this t-degree polynomial A (X).

And now, suppose I instruct every party that, okay, you take your respective share of the unknown value s and multiply it with some publicly known element c, public constant c; it is known to everyone. The constant c is known to everyone. Now, if I instruct every party to do this, and now since the dot operation of the field satisfies the closure property, after performing the dot operation on their respective shares, we will again obtain a vector of field elements, where the ith component of the vector will be available with the ith party. Let us call the resultant uh product elements as $v_1$to v_n. Now, what can I say about this new vector of n values v_1 to v_n?

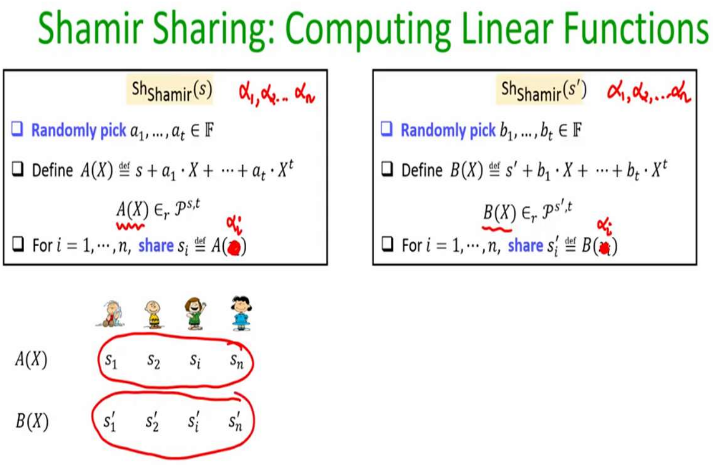
Is it an arbitrary vector of n field element or does it constitute a special vector? Again, it turns out that it constitutes a special vector of n values. Namely, these vectors constitute an n, t Shamir secret-sharing of the value c * s. Why so? Because, A(X) was a polynomial of degree-t, and its constant term was s. Now, consider the polynomial c * A(X). Its degree also will be t, because you are just multiplying each coefficient of the A(X) polynomial by a field element.

And as a result, you will, the coefficient just will change, but you will still have uh terms from x^0 to x^t; so, that is why its degree will be t. And what can I say about the (const) so, let uh let us call this polynomial as uh U(X) polynomial. So, U(X) polynomial is a t-degree polynomial. And what can I say about the constant term of this U polynomial? The constant term of this U polynomial is c * A$_0$.

And A$_0$ is nothing but my secret s; so, it is nothing but c *s. So, that means, by multiplying their respective shares of the unknown value s with this public constant c, the parties will obtain another set of shares which will actually constitute a vector of Shamir shares for the element c *s. That means, as if the value c * s has been now secret-shared among the parties.

And moreover, if this vector of shares for the secret s was random; vector is random in the sense that, if this A(X) polynomial was randomly chosen from the set of all possible t-degree polynomials whose constant term is s, then so is the U(X) polynomial. So, if A(X) polynomial was a random element from the set of all possible polynomials of degree-t with constant term s, then I can claim that the polynomial U(X), which will be the product of the c and A(X) polynomial is also a random element from the set of all possible t-degree polynomials whose constant term is c * s. I stress, in both operations, the value of s is not revealed, parties are not performing any interaction among themselves, they are just applying the operation locally on their shares of s.

(Refer Slide Time: 21:45)



Shamir Sharing: Computing Linear Functions

$\mathsf{Sh}_{\mathsf{Shamir}}(s)$ $\alpha_1, \alpha_2 .. \alpha_n$

❑ Randomly pick $a_1, \dots, a_t \in \mathbb{F}$

❑ Define $A(X) \overset{\text{def}}{=} s + a_1 \cdot X + \cdots + a_t \cdot X^t$

$A(X) \in_r \mathcal{P}^{s,t}$

❑ For $i = 1, \cdots, n$, share $s_i \overset{\text{def}}{=} A(\overset{\alpha_i}{\bullet})$

$\mathsf{Sh}_{\mathsf{Shamir}}(s')$ $\alpha_1, \alpha_2, .. \alpha_n$

❑ Randomly pick $b_1, \dots, b_t \in \mathbb{F}$

❑ Define $B(X) \overset{\text{def}}{=} s' + b_1 \cdot X + \cdots + b_t \cdot X^t$

$B(X) \in_r \mathcal{P}^{s',t}$

❑ For $i = 1, \cdots, n$, share $s'_i \overset{\text{def}}{=} B(\overset{\alpha_i}{\bullet})$

$A(X)$ s_1 s_2 s_i s_n

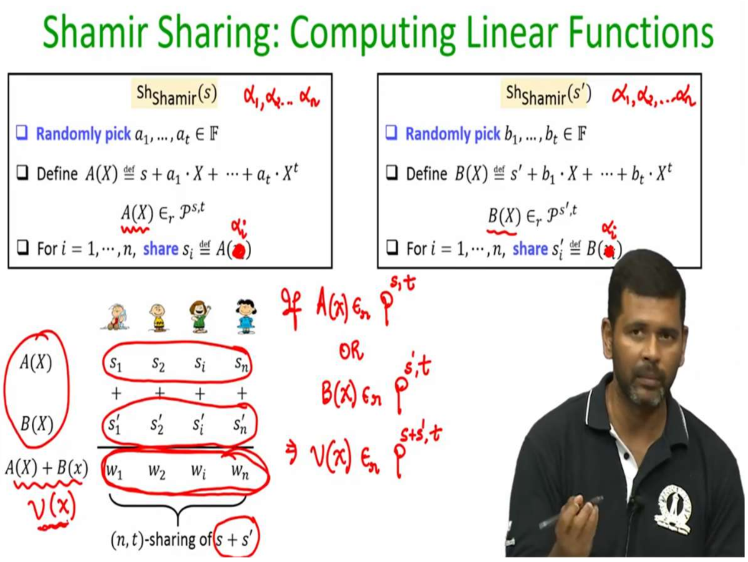
$B(X)$ s'_1 s'_2 s'_i s'_n

Now, let us see some another magic. Imagine that there are 2 independent values s and s'which are secret-shared among the parties P$_1$ to P$_n$. Again, let us call thisα_i here and α_i here. That means, in both the instances the shares are computed by evaluating the sharing polynomial at the same fixed

α_1 to α_n. That means, for secret-sharing the value s, a random polynomial of degree-t whose constant term would have been a was picked; and that polynomial was evaluated atα_1 to α_n, resulting in this vector of shares.

And for evaluating the secret s', a random polynomial B(X) was picked, whose constant term is s' and degree was t; and that polynomial was evaluated at α_1 to α_n, resulting in this vector of shares.

(Refer Slide Time: 22:57)



Shamir Sharing: Computing Linear Functions

$\mathsf{Sh}_{\mathsf{Shamir}}(s)$

- □ Randomly pick $a_1, \dots, a_t \in \mathbb{F}$
- □ Define $A(X) \overset{\text{def}}{=} s + a_1 \cdot X + \cdots + a_t \cdot X^t$

  $A(X) \in_r \mathcal{P}^{s,t}$
- □ For $i = 1, \cdots, n$, share $s_i \overset{\text{def}}{=} A(\alpha_i)$

$\mathsf{Sh}_{\mathsf{Shamir}}(s')$

- □ Randomly pick $b_1, \dots, b_t \in \mathbb{F}$
- □ Define $B(X) \overset{\text{def}}{=} s' + b_1 \cdot X + \cdots + b_t \cdot X^t$

  $B(X) \in_r \mathcal{P}^{s',t}$
- □ For $i = 1, \cdots, n$, share $s'_i \overset{\text{def}}{=} B(\alpha_i)$

$\alpha_1, \alpha_2 .. \alpha_n$
$\alpha_1, \alpha_2, ... \alpha_n$
α_i
α_i
$A(X)$
$B(X)$
$A(X) + B(x)$
$V(x)$
s_1 s_2 s_i s_n
+ + + +
s'_1 s'_2 s'_i s'_n
w_1 w_2 w_i w_n
(n, t)-sharing of $s + s'$
If $A(x) \in_r P^{s,t}$
OR
$B(x) \in_r P^{s',t}$
$\Rightarrow V(x) \in_r P^{s+s',t}$

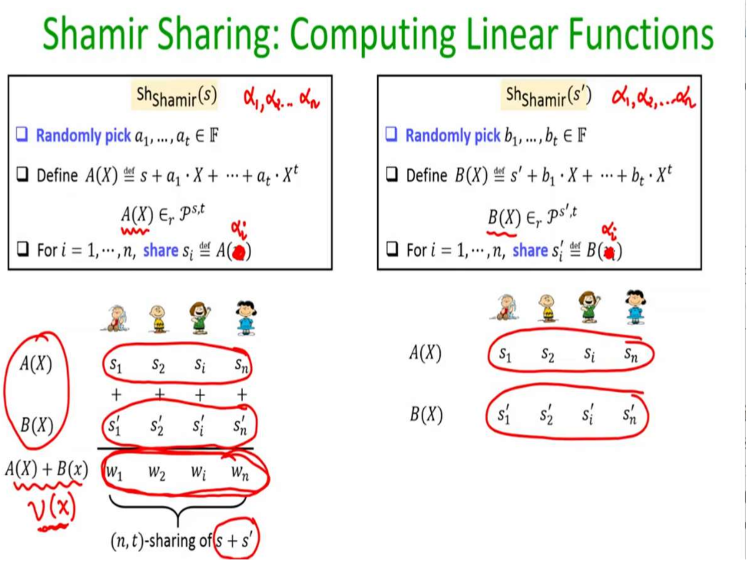
Now, imagine that each party adds its respective shares of s and s'. Since the + operation is satisfying the closure property, they will obtain another set of field elements as a whole. So, this will be now, the new vector of n field elements. And now, if you see closely here, this new vector of n field elements actually constitutes a set of (n, t) shares, Shamir shares for the secret s + s'.

This is because, if I consider the polynomial A(X) + B (x); let us call that polynomial as V of X polynomial. Now, this V of X polynomial will have degree-t, because A(X) is a t-degree polynomial, B(X) is a t-degree polynomial; hence its summation also we will be a t-degree polynomial. And the constant term of this V polynomial will be the summation of the constant terms of the A polynomial and the B polynomial, namely s and s'.

So, that means, I can imagine as if this w 1 to w n is a vector of n values, which would have been obtained if the secret s + s'would have been shared by picking this polynomial V of X. And, again we get the property that, if A(X) was randomly chosen from the set of all possible polynomials of degree-t with constant term s, or B(X) was randomly chosen; that means, if any of these 2 vectors of n, t's shares, either the shares of s or the shares of s'were random vector of shares, then I can conclude that, this V of X also constitutes a vector of random n shares for the secret s + s'.

Because, if at least 1 of these 2 polynomials A(X) or B(X) was randomly chosen, then so is the V of X polynomial. So, that means, what we have seen till now is that there are certain operations which can be performed over the underlying shared value without knowing them, by performing the same operations on the shares themselves.

(Refer Slide Time: 25:49)



Shamir Sharing: Computing Linear Functions

$\mathsf{Sh}_{\mathsf{Shamir}}(s)$ $\alpha_1, \alpha_2 .. \alpha_n$

- ❑ Randomly pick $a_1, \ldots, a_t \in \mathbb{F}$
- ❑ Define $A(X) \stackrel{\text{def}}{=} s + a_1 \cdot X + \cdots + a_t \cdot X^t$

$A(X) \in_r \mathcal{P}^{s,t}$

- ❑ For $i = 1, \cdots, n$, share $s_i \stackrel{\text{def}}{=} A(\alpha_i)$

$\mathsf{Sh}_{\mathsf{Shamir}}(s')$ $\alpha_1, \alpha_2, \ldots \alpha_n$

- ❑ Randomly pick $b_1, \ldots, b_t \in \mathbb{F}$
- ❑ Define $B(X) \stackrel{\text{def}}{=} s' + b_1 \cdot X + \cdots + b_t \cdot X^t$

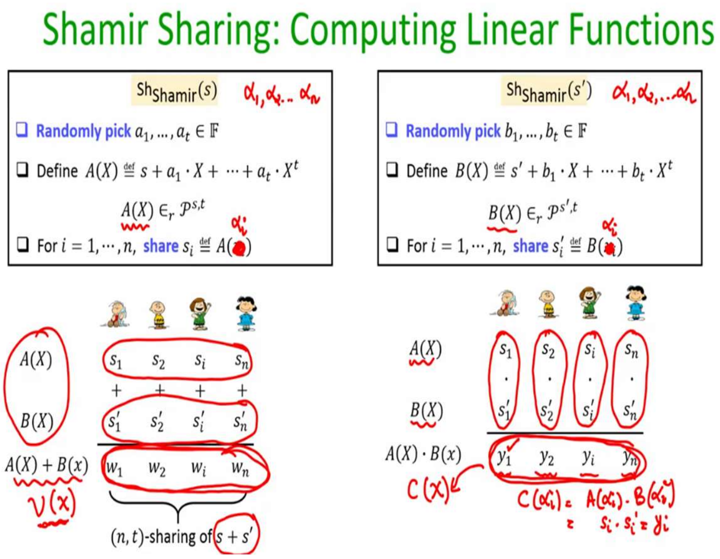
$B(X) \in_r \mathcal{P}^{s',t}$

- ❑ For $i = 1, \cdots, n$, share $s'_i \stackrel{\text{def}}{=} B(\alpha_i)$

$A(X)$ s_1 s_2 s_i s_n
+ + + +
$B(X)$ s'_1 s'_2 s'_i s'_n
$A(X) + B(x)$ w_1 w_2 w_i w_n
$v(x)$
(n,t)-sharing of $s + s'$
$A(X)$ s_1 s_2 s_i s_n
$B(X)$ s'_1 s'_2 s'_i s'_n

Now, what about the multiplication of s and s'? So, imagine s for secret-shared and this was the vector of shares; and s'is also secret-shared. Parties do not know the value of s; parties do not know the value of s'; but they would like to compute shares of s * s'. So, again, based on whatever we have seen till now, you might be tempted to propose that, why not let each party multiply locally its share of s and its share of s'?

(Refer Slide Time: 26:24)



Shamir Sharing: Computing Linear Functions

$\mathsf{Sh}_{\mathsf{Shamir}}(s)$ $\alpha_1, \alpha_2 .. \alpha_n$

□ Randomly pick $a_1, \ldots, a_t \in \mathbb{F}$

□ Define $A(X) \overset{\text{def}}{=} s + a_1 \cdot X + \cdots + a_t \cdot X^t$

$A(X) \in_r \mathcal{P}^{s,t}$

□ For $i = 1, \cdots, n$, share $s_i \overset{\text{def}}{=} A(\alpha_i)$

$\mathsf{Sh}_{\mathsf{Shamir}}(s')$ $\alpha_1, \alpha_2, .. \alpha_n$

□ Randomly pick $b_1, \ldots, b_t \in \mathbb{F}$

□ Define $B(X) \overset{\text{def}}{=} s' + b_1 \cdot X + \cdots + b_t \cdot X^t$

$B(X) \in_r \mathcal{P}^{s',t}$

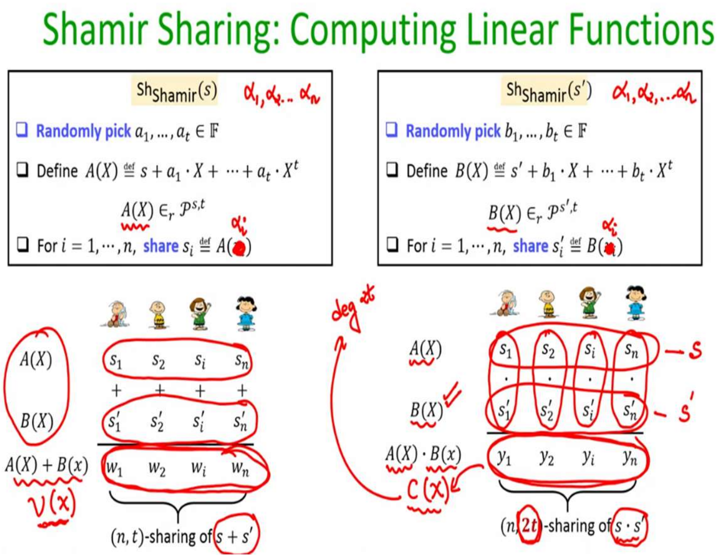
□ For $i = 1, \cdots, n$, share $s'_i \overset{\text{def}}{=} B(\alpha_i)$

$A(X)$
$B(X)$
s_1 s_2 s_i s_n
+ + + +
s'_1 s'_2 s'_i s'_n
$A(X) + B(x)$
w_1 w_2 w_i w_n
$V(x)$
(n, t)-sharing of $s + s'$
$A(X)$
$B(X)$
$A(X) \cdot B(x)$
$s_1 \cdot s'_1$ $s_2 \cdot s'_2$ $s_i \cdot s'_i$ $s_n \cdot s'_n$
y_1 y_2 y_i y_n
$C(x)$
$C(\alpha_i) = A(\alpha_i) \cdot B(\alpha_i)$
$= s_i \cdot s'_i = y_i$

So, let us do that. So, let us propose the following. Each party, say party P $_1$, takes its share of s and its share of s', and it multiplies them and obtain a new value, call it y $_1$. Similarly, P $_2$, it takes its share of s and its share of s', multiply them and it gets a value y $_2$, and so on. So, like that, every party is doing that. Now, what can I say about the vector of this new n values? Do they constitute Shamir shares of the secret s * s'?

So, if I consider the product of these 2 polynomials A(X) and B(X); let us call that polynomial as mm c(x) polynomial. Now, c(x) polynomial evaluated at alpha 1 will give you y 1, because C of alpha i will be equal to A of alpha i into B of alpha i. A of alpha i is s i, the ith share of the value s; B of Alpha i is the ith share of s', namely s i prime. And as per the multiplication operation that each party has performed, this is nothing but y of i. So, that means, indeed, these values y 1 to y n, they lie on the polynomial c(x) at X equal to alpha 1, X equal to alpha 2, X equal to alpha n; fine.

(Refer Slide Time: 28:08)



Shamir Sharing: Computing Linear Functions

$\mathsf{Sh}_{\mathsf{Shamir}}(s)$ $\alpha_1, \alpha_2 .. \alpha_n$

❑ Randomly pick $a_1, \ldots, a_t \in \mathbb{F}$

❑ Define $A(X) \overset{\text{def}}{=} s + a_1 \cdot X + \cdots + a_t \cdot X^t$

$A(X) \in_r \mathcal{P}^{s,t}$

❑ For $i = 1, \cdots, n$, share $s_i \overset{\text{def}}{=} A(\overset{\alpha_i}{\bullet})$

$\mathsf{Sh}_{\mathsf{Shamir}}(s')$ $\alpha_1, \alpha_2, \ldots \alpha_n$

❑ Randomly pick $b_1, \ldots, b_t \in \mathbb{F}$

❑ Define $B(X) \overset{\text{def}}{=} s' + b_1 \cdot X + \cdots + b_t \cdot X^t$

$B(X) \in_r \mathcal{P}^{s',t}$

❑ For $i = 1, \cdots, n$, share $s'_i \overset{\text{def}}{=} B(\overset{\alpha_i}{\bullet})$

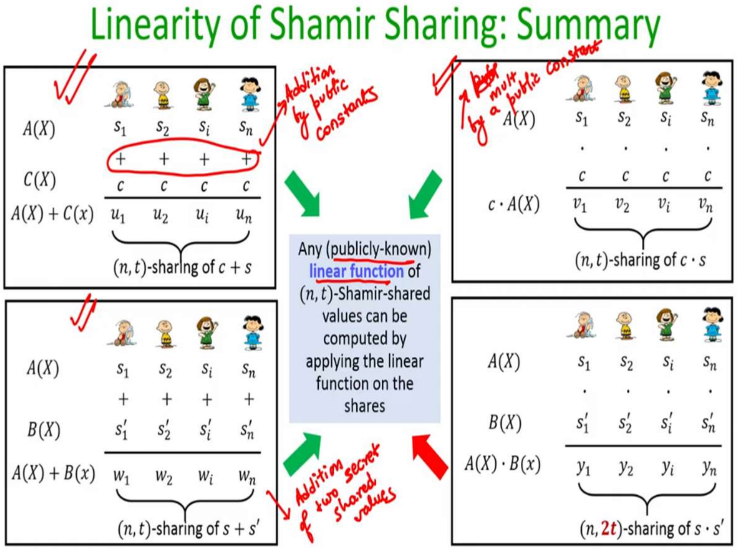
But what is the degree of this c(x) polynomial? The degree of this c(x) polynomial is no longer t, because it is now the product of two t-degree polynomials. And if I multiply two t-degree polynomials, the degree of c(x) becomes 2t; it is no longer t. That means, this new vector of n values, it indeed constitutes shares of s * s'. But, the degree of sharing is no longer t, but rather it is 2t.

But, this was not the case for the earlier operations, right? For the earlier operations, when I performed the operations on the shares, I still obtained a new vector of shares, where the degree of sharing was still t. But now, the degree of sharing has changed from t to 2t. What does it mean that the degree is 2t? It means that, in order to reconstruct the value s * s', it is no longer the case that any set of t + 1 shareholders can come together and reconstruct it.

So, we started with a t sharing or n, t sharing of the values. That means, the secret s was shared in such a way that any group of t + 1 shareholders could come together and reconstruct the value s, because they constitute an authorised set. Similarly, the secret s'was shared in such a way that any group of t + 1 parties could come together and reconstruct this polynomial B of X.

But now, if parties locally multiply their shares of s and s'and obtain their shares of s into s'; to reconstruct the value s into s', we now need 2t + 1 or more number of shareholders to come together, and then only they can reconstruct back this polynomial c(x). If just a set of t + 1 shareholders come together, they can no longer reconstruct it.

(Refer Slide Time: 30:30)



Linearity of Shamir Sharing: Summary

$A(X)$	s_1	s_2	s_i	s_n
	$+$	$+$	$+$	$+$
$C(X)$	c	c	c	c
$A(X)+C(x)$	u_1	u_2	u_i	u_n

(n,t)-sharing of $c+s$

Addition by public constants

$A(X)$	s_1	s_2	s_i	s_n
	$\cdot$	$\cdot$	$\cdot$	$\cdot$
	c	c	c	c
$c \cdot A(X)$	v_1	v_2	v_i	v_n

(n,t)-sharing of $c \cdot s$

~~Best~~ mult by a public constant

Any (publicly-known) linear function of (n,t)-Shamir-shared values can be computed by applying the linear function on the shares

$A(X)$	s_1	s_2	s_i	s_n
	$+$	$+$	$+$	$+$
$B(X)$	s'_1	s'_2	s'_i	s'_n
$A(X)+B(x)$	w_1	w_2	w_i	w_n

(n,t)-sharing of $s+s'$

Addition of two secret shared values

$A(X)$	s_1	s_2	s_i	s_n
	$\cdot$	$\cdot$	$\cdot$	$\cdot$
$B(X)$	s'_1	s'_2	s'_i	s'_n
$A(X) \cdot B(x)$	y_1	y_2	y_i	y_n

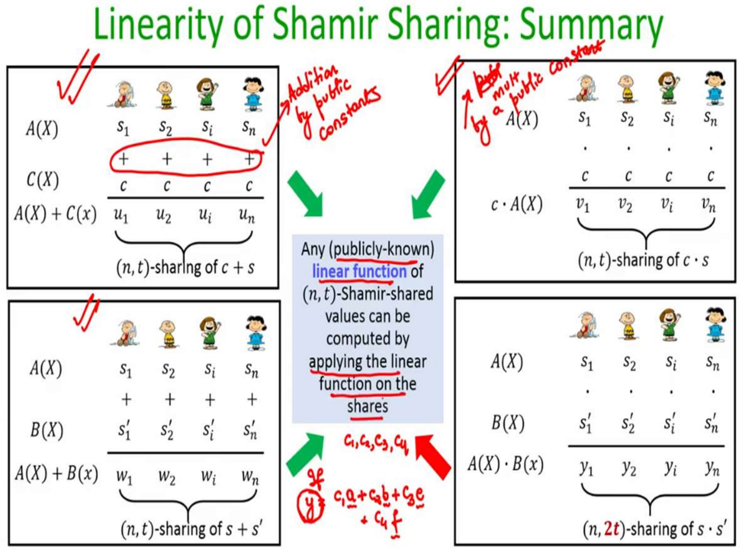
$(n,2t)$-sharing of $s \cdot s'$

So, let me summarise the linearity property of Shamir sharing. We have seen some operations which we can perform on secret-shared values, namely, we have seen addition by public constants. So, this was the addition by public constant operation. This is the addition of two secret-shared values. This was the multiplication by a public constant. So, these three operations, this operation, this operation and this operation satisfies the linearity property.

That means, you started with some secret-shared value and you want to either add a constant element or multiply the secret-shared value with some constant element or you want to add two unknown secret-shared values; all of them can be performed locally. Namely, you just apply the same operation which you want to perform on the underlying shared value, on the shares themselves, and you obtain the shares of the result that you would have obtained or you would have desired on the secret-shared value.

But when it comes to multiplying two secret-shared values, that is not possible by just locally multiplying the shares of the secret-shared values. So, what does it tell you, this entire set of linearity operations? So, it tells you that, if you have any publicly known linear function of some shared values, then the result of that publicly known linear function can be obtained in a secret-shared fashion by applying the linear function on the shares themselves. So, for instance, what I am saying here is the following:

(Refer Slide Time: 32:59)



Linearity of Shamir Sharing: Summary

$A(X)$: s_1 s_2 s_i s_n

$+$ $+$ $+$ $+$

$C(X)$: c c c c

$A(X)+C(x)$: u_1 u_2 u_i u_n

(n,t)-sharing of $c+s$

Addition by public constants

$A(X)$: s_1 s_2 s_i s_n

$\cdot$ $\cdot$ $\cdot$ $\cdot$

c c c c

$c \cdot A(X)$: v_1 v_2 v_i v_n

(n,t)-sharing of $c \cdot s$

~~Both~~ mult by a public constant

Any (publicly-known) linear function of (n,t)-Shamir-shared values can be computed by applying the linear function on the shares

c_1, c_2, c_3, c_4

if $y = c_1 a + c_2 b + c_3 e + c_4 f$

$A(X)$: s_1 s_2 s_i s_n

$+$ $+$ $+$ $+$

$B(X)$: s_1' s_2' s_i' s_n'

$A(X)+B(x)$: w_1 w_2 w_i w_n

(n,t)-sharing of $s+s'$

$A(X)$: s_1 s_2 s_i s_n

$\cdot$ $\cdot$ $\cdot$ $\cdot$

$B(X)$: s_1' s_2' s_i' s_n'

$A(X)\cdot B(x)$: y_1 y_2 y_i y_n

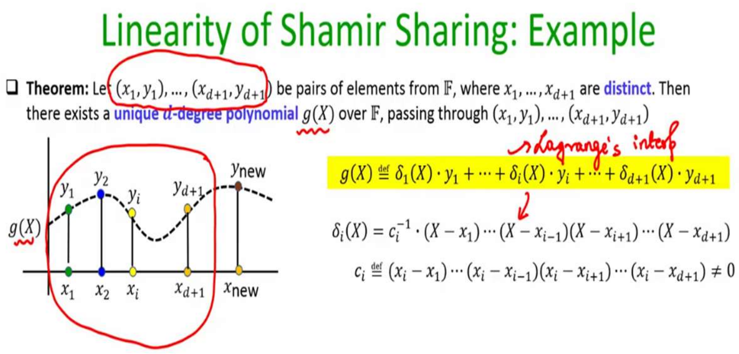
$(n,2t)$-sharing of $s \cdot s'$

If you have a function of the following form; if say y is equal to, say some constant * a + another constant * b + some another constant time, say e, and say another constant * f. If this is the case, if this is the function you want to compute, and suppose you do not want to reveal the values of a, b, e and f. The constants c_1, c_2, c_3, c_4, they are publicly known, but the values a, b, e and f, they are not publicly known, but rather they are available in a secret-shared fashion.

That means, each party has a share of a; each party has a share of b; each party has a share of e; and each party has a share of f; where the shares would have been computed by Shamir secret-sharing. Now, my claim is that, if this is the setting given to you, then by asking each party to multiply their shares of a with c_1, and multiplying their shares of b with c_2, and then multiplying their shares of e with c_3 and multiplying their shares of f with c_4, and then adding all the resultant values, we actually will obtain a vector of n shares, which constitutes a Shamir secret-sharing of the value y.

That means, it is fine even if you do not know the value a, b, e and f. By performing some operations on the shares of a, b, e and f, you would have obtained shares of y. That is what is the linearity property of Shamir secret-sharing. It allows you to compute any linear function of secret-shared values by applying the linear function on the shares themselves.

(Refer Slide Time: 35:02)



Linearity of Shamir Sharing: Example

❑ **Theorem:** Let $(x_1, y_1), \ldots, (x_{d+1}, y_{d+1})$ be pairs of elements from $\mathbb{F}$, where $x_1, \ldots, x_{d+1}$ are **distinct**. Then there exists a **unique d-degree polynomial** $g(X)$ over $\mathbb{F}$, passing through $(x_1, y_1), \ldots, (x_{d+1}, y_{d+1})$

→ Lagrange's interp

$$g(X) \overset{\text{def}}{=} \delta_1(X) \cdot y_1 + \cdots + \delta_i(X) \cdot y_i + \cdots + \delta_{d+1}(X) \cdot y_{d+1}$$

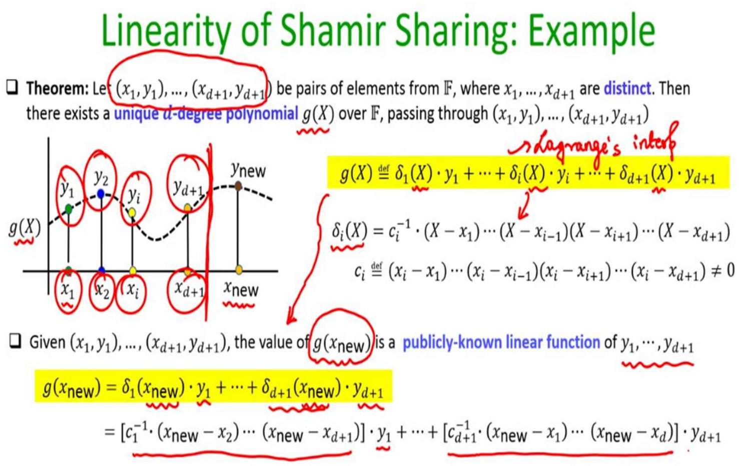
$$\delta_i(X) = c_i^{-1} \cdot (X - x_1) \cdots (X - x_{i-1})(X - x_{i+1}) \cdots (X - x_{d+1})$$

$$c_i \overset{\text{def}}{=} (x_i - x_1) \cdots (x_i - x_{i-1})(x_i - x_{i+1}) \cdots (x_i - x_{d+1}) \neq 0$$

So, let us see an example for this, where this will be useful? And we will require this specific example later. So, here, the setting is as follows: You are given d + 1 distinct points in the two-dimensional plane over the field. And if that is the case, then we know that there exists a unique d-degree polynomial g(X) passing through those d + 1 distinct points. So, these are the d + 1 distinct points given to you.

So, there would be some curve g(X) passing through this d + 1 distinct points, which we can obtain as per the Lagrange's interpolation formula. And if I expand this Lagrange's interpolation formula, as we have seen in the earlier lecture, this will be the value of the ith delta polynomial. It will have all the elements except x $_i$ as its roots. And as a result, it will vanish if I substitute X equal to x $_1$, x$_2$, x $_{i \text{ minus } 1}$, x $_{i+1}$, and so on. And it will survive at x equal to x $_i$.

(Refer Slide Time: 36:29)



Linearity of Shamir Sharing: Example

❑ **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** $g(X)$ over $\mathbb{F}$, passing through $(x_1, y_1), \dots, (x_{d+1}, y_{d+1})$

→ Lagrange's interp

$$g(X) \overset{\text{def}}{=} \delta_1(X) \cdot y_1 + \cdots + \delta_i(X) \cdot y_i + \cdots + \delta_{d+1}(X) \cdot y_{d+1}$$

$$\delta_i(X) = c_i^{-1} \cdot (X - x_1) \cdots (X - x_{i-1})(X - x_{i+1}) \cdots (X - x_{d+1})$$

$$c_i \overset{\text{def}}{=} (x_i - x_1) \cdots (x_i - x_{i-1})(x_i - x_{i+1}) \cdots (x_i - x_{d+1}) \neq 0$$

❑ Given $(x_1, y_1), \dots, (x_{d+1}, y_{d+1})$, the value of $g(x_{\text{new}})$ is a **publicly-known linear function** of $y_1, \cdots, y_{d+1}$

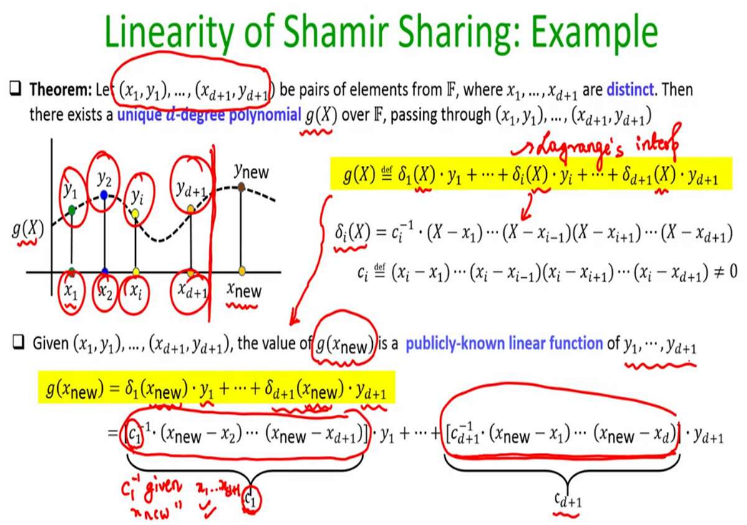
$$g(x_{\text{new}}) = \delta_1(x_{\text{new}}) \cdot y_1 + \cdots + \delta_{d+1}(x_{\text{new}}) \cdot y_{d+1}$$

$$= [c_1^{-1} \cdot (x_{\text{new}} - x_2) \cdots (x_{\text{new}} - x_{d+1})] \cdot y_1 + \cdots + [c_{d+1}^{-1} \cdot (x_{\text{new}} - x_1) \cdots (x_{\text{new}} - x_d)] \cdot y_{d+1}$$

Now, imagine there is a new value of x, x new, which is different from all the previous x coordinates x $_{1,}$ x $_2$, x $_{d+1}$. And I want to compute the value of this g polynomial at X equal to x new. My claim is that the value of this polynomial g at X equal to x new is a linear function of the existing y values and the existing x values. Why so? Because, if this is my g polynomial, then to compute the value of this g polynomial at X equal to x new, I just have to substitute X equal to x new everywhere, in all the delta polynomials.

So, that is what I have done. At all the delta polynomials, I have substitute X equal to x new. And now, I know the value of each delta polynomial. So, if I take the first delta polynomial and there if I substitute X equal to x new, I will obtain this value; multiplied with y_1, that is outside. In the second delta polynomial, if I substitute X equal to x new, I will obtain another value multiplied with y_2. And then finally, if I take the last delta polynomial, there if I substitute X equal to x new, I will obtain this value. And that has to be multiplied with y $_{d+1}$.

(Refer Slide Time: 38:09)



Linearity of Shamir Sharing: Example

- □ **Theorem:** Let $(x_1, y_1), \ldots, (x_{d+1}, y_{d+1})$ be pairs of elements from $\mathbb{F}$, where $x_1, \ldots, x_{d+1}$ are distinct. Then there exists a unique d-degree polynomial $g(X)$ over $\mathbb{F}$, passing through $(x_1, y_1), \ldots, (x_{d+1}, y_{d+1})$

→Lagrange's interp

$$g(X) \overset{\text{def}}{=} \delta_1(X) \cdot y_1 + \cdots + \delta_i(X) \cdot y_i + \cdots + \delta_{d+1}(X) \cdot y_{d+1}$$

$$\delta_i(X) = c_i^{-1} \cdot (X - x_1) \cdots (X - x_{i-1})(X - x_{i+1}) \cdots (X - x_{d+1})$$

$$c_i \overset{\text{def}}{=} (x_i - x_1) \cdots (x_i - x_{i-1})(x_i - x_{i+1}) \cdots (x_i - x_{d+1}) \neq 0$$

- □ Given $(x_1, y_1), \ldots, (x_{d+1}, y_{d+1})$, the value of $g(x_{\text{new}})$ is a publicly-known linear function of $y_1, \cdots, y_{d+1}$

$$g(x_{\text{new}}) = \delta_1(x_{\text{new}}) \cdot y_1 + \cdots + \delta_{d+1}(x_{\text{new}}) \cdot y_{d+1}$$

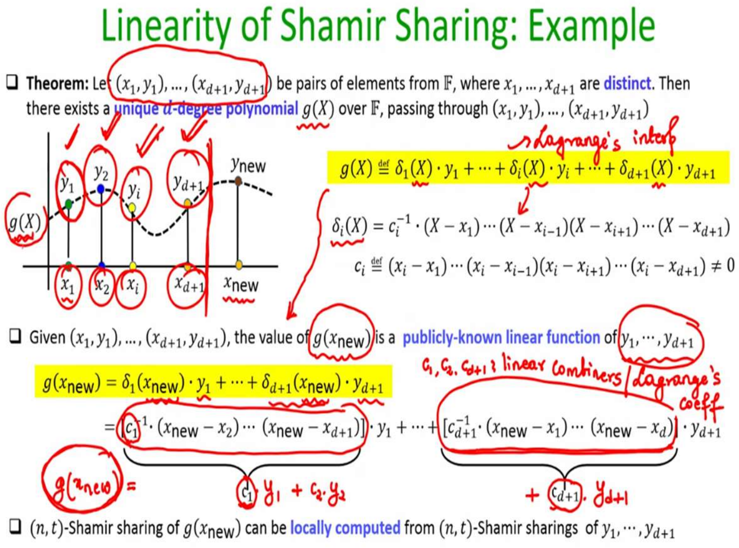
$$= \underbrace{[c_1^{-1} \cdot (x_{\text{new}} - x_2) \cdots (x_{\text{new}} - x_{d+1})]}_{c_1} \cdot y_1 + \cdots + \underbrace{[c_{d+1}^{-1} \cdot (x_{\text{new}} - x_1) \cdots (x_{\text{new}} - x_d)]}_{c_{d+1}} \cdot y_{d+1}$$

c_1^{-1} given
"x_{new}"
$x_1 \ldots x_{d+1}$ ✓ ✓

So, now, if you see closely here, I can call this term, whatever is there in this square bracket, as c $_1$. This c $_1$ is different from this c $_1$; so, that is why a different font; this is a new constant. And why it is a constant? It is a constant because, c 1 inverse is given, it is publicly known; and x new is given; and all the values of old x's, namely x $_1$ to x $_{d+1}$, they are also given.

So, that is why, the result of performing the operation inside the square bracket, whatever is the result, that will be a field element, but that will be publicly known; so, I can consider it as a constant. So, let me call it constant c $_1$. In the same way, whatever is there inside the d + 1th square bracket, the result of that operation, I am denoting it by c $_{d+1}$, which is a constant; because everything inside the d + 1 th square bracket is publicly known.

(Refer Slide Time: 39:25)



Linearity of Shamir Sharing: Example

□ **Theorem:** Let $(x_1, y_1), \ldots, (x_{d+1}, y_{d+1})$ be pairs of elements from $\mathbb{F}$, where $x_1, \ldots, x_{d+1}$ are distinct. Then there exists a unique d-degree polynomial $g(X)$ over $\mathbb{F}$, passing through $(x_1, y_1), \ldots, (x_{d+1}, y_{d+1})$

Lagrange's interp

$$g(X) \overset{\text{def}}{=} \delta_1(X) \cdot y_1 + \cdots + \delta_i(X) \cdot y_i + \cdots + \delta_{d+1}(X) \cdot y_{d+1}$$

$$\delta_i(X) = c_i^{-1} \cdot (X - x_1) \cdots (X - x_{i-1})(X - x_{i+1}) \cdots (X - x_{d+1})$$

$$c_i \overset{\text{def}}{=} (x_i - x_1) \cdots (x_i - x_{i-1})(x_i - x_{i+1}) \cdots (x_i - x_{d+1}) \neq 0$$

□ Given $(x_1, y_1), \ldots, (x_{d+1}, y_{d+1})$, the value of $g(x_{\text{new}})$ is a publicly-known linear function of $y_1, \cdots, y_{d+1}$

c_1, c_2, c_{d+1} : linear combiners / Lagrange's coeff

$$g(x_{\text{new}}) = \delta_1(x_{\text{new}}) \cdot y_1 + \cdots + \delta_{d+1}(x_{\text{new}}) \cdot y_{d+1}$$

$$= \underbrace{[c_1^{-1} \cdot (x_{\text{new}} - x_2) \cdots (x_{\text{new}} - x_{d+1})]}_{c_1} \cdot y_1 + \cdots + \underbrace{[c_{d+1}^{-1} \cdot (x_{\text{new}} - x_1) \cdots (x_{\text{new}} - x_d)]}_{c_{d+1}} \cdot y_{d+1}$$

$g(x_{new}) = c_1 y_1 + c_2 \cdot y_2 + c_{d+1} \cdot y_{d+1}$

□ (n, t)-Shamir sharing of $g(x_{\text{new}})$ can be locally computed from (n, t)-Shamir sharings of $y_1, \cdots, y_{d+1}$

And then, I can imagine now that my g(X) new is equal to this constant * y_1 + second constant * y_2, and like that, the d + 1th constant * y_{d+1}, which is precisely a form of a linear function. That means, g(X) new is basically a linear function of y_1 to y_{d+1}, where this c_1, c_2, c_{d+1} are your linear combiners and they are publicly known.

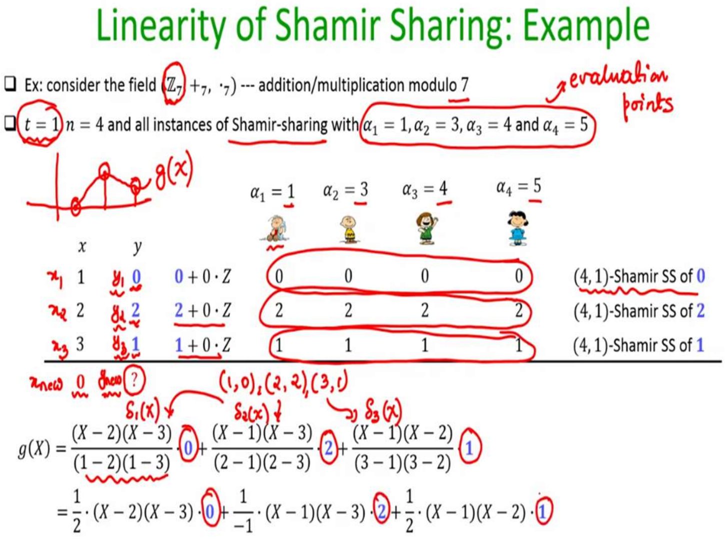
So, these linear combiners c_1, this fancy c_1, fancy looking c_2, fancy looking c'_{d+1}, they are the linear combiners, and some times, they are often called as Lagrange's coefficients. So, the point here is that, if you want to compute the value of g curve at x new, that can be expressed as a linear combination of the existing values on the g polynomial. The existing values were y_1, y_2, y_i, $y_{(d+1)}$.

If they are given to you, then, any new point on this g curve can be expressed as a linear combination of the existing d + 1 points on that g curve. Now, imagine a setting where you are not given the exact value of y_1, but each party is given a share of y_1 as per the Shamir secret-sharing. That means, the value y_1 is not available in the clear, but it is secret-shared. In the same way, the value y_2 is secret-shared, value y_i is secret-shared and value $y_{(d+1)}$ is also secret-shared.

x_1, x_2, $x_{(d+1)}$, they are not secret-shared, they are publicly known; but the y components, they are secret-shared individually, among the n parties. If that is the setting given to you, my claim is, you can compute the value of g polynomial at x new also in the secret-shared fashion. That means, no one will learn the value of the g polynomial at x new, but they can perform some operation on the shares of y1, y2, yi, y(d+1), which will give them shares of g(X) new, as per Shamir secret-sharing.

And this is like a magic, because even without knowing the full curve g(X); in this whole process, that curve g(X) will not be constructed, but rather you will be magically able to compute shares of g(X) new.

(Refer Slide Time: 42:35)



Linearity of Shamir Sharing: Example

- ❑ Ex: consider the field $(\mathbb{Z}_7, +_7, \cdot_7)$ --- addition/multiplication modulo 7
- ❑ $t = 1$, $n = 4$ and all instances of Shamir-sharing with $\alpha_1 = 1, \alpha_2 = 3, \alpha_3 = 4$ and $\alpha_4 = 5$

	x	y		$\alpha_1 = 1$	$\alpha_2 = 3$	$\alpha_3 = 4$	$\alpha_4 = 5$	
x_1	1	y_1 0	$0 + 0 \cdot Z$	0	0	0	0	(4, 1)-Shamir SS of 0
x_2	2	y_2 2	$2 + 0 \cdot Z$	2	2	2	2	(4, 1)-Shamir SS of 2
x_3	3	y_3 1	$1 + 0 \cdot Z$	1	1	1	1	(4, 1)-Shamir SS of 1
x_{new}	0	y_{new} ?						

$$g(X) = \underbrace{\frac{(X-2)(X-3)}{(1-2)(1-3)}}_{\delta_1(x)} \cdot 0 + \underbrace{\frac{(X-1)(X-3)}{(2-1)(2-3)}}_{\delta_2(x)} \cdot 2 + \underbrace{\frac{(X-1)(X-2)}{(3-1)(3-2)}}_{\delta_3(x)} \cdot 1$$

$$= \frac{1}{2} \cdot (X-2)(X-3) \cdot 0 + \frac{1}{-1} \cdot (X-1)(X-3) \cdot 2 + \frac{1}{2} \cdot (X-1)(X-2) \cdot 1$$

So, let me demonstrate that with an example here. So, I take a field Z 7, where all the addition and multiplication operations are performed modulo 7. Let us consider a case where t = 1, namely, all the values are secret-shared with degree of sharing being 1, namely, all the values will be shared through a straight line. And suppose there are n parties and say these are my evaluation points for Shamir secret-sharing.

That means, the shares of first party for all the values in the system will be computed by evaluating the underlying straight line at alpha 1 and so on. So, you can see that I am free to choose any 4 distinct non-zero elements, I have not selected alpha 2 to be 2, I have purposely selected alpha 2 to be 3. So, the point is, alpha 1, alpha 2, alpha 3, alpha 4, they can be any 4 distinct non-zero elements from this field, that is all.

So, now, imagine that my x_1, x_2 and x_3, they are 1, 2, 3 and say the corresponding y values are 0, 2 and 1. So, I have denoted the corresponding y values in colour, because they are not available with any single party, but rather the value 0, 2 and 1, they are secret-shared among these 4 parties by instances of Shamir secret-sharing with the degree of sharing being 1. So, imagine that the value is 0 is shared through the straight line 0 + 0 Z.

That is a straight line equation. It is fine that the coefficient of Z is 0; that is fine. But overall, this can be interpreted as a straight line. And now, this straight line evaluated at 1, 3, 4 and 5, will give you the shares 0, 0, 0, 0. That means, I can imagine that this is now a vector of 4, 1 Shamir shares of the value 0. In the same way, imagine that the value 2 is secret-shared through this straight line; and that straight line evaluated at alpha 1, alpha 2, alpha 3, alpha 4, gives you these values.

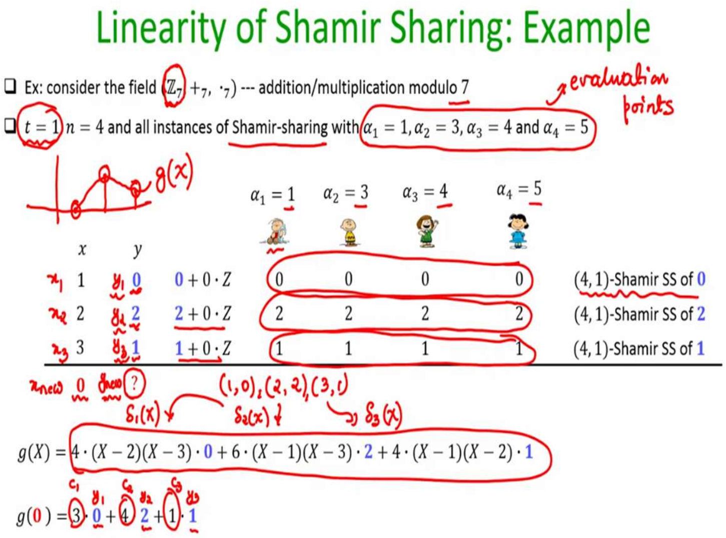
And imagine that the value 1 is shared through this straight line; and that straight line evaluated at alpha 1, alpha 2, alpha 3, alpha 4, gives you these vector of shares. That is a setting given to you. That means, if any 1 of these 4 parties is curious and trying to find out what is the value of y_1, y_2 and y_3, it cannot find out as per the property of Shamir secret-sharing.

So, that means, I am basically now talking about a curve passing through 1, 0. That means, at 1, it evaluates to 0; at 2, it evaluates to 2 say; this is the point; and at 3, it evaluates to 1; say, some curve; so, this is not the precise curve. And I now want to evaluate that curve at x = 0, and compute the shares of the resultant y value. So, this is my x new. I want to compute shares of y new.

And in the whole process, nothing about y_1, y_2 and y_3 should be revealed; just somehow we want to ensure that y new's shares are computed. So, let us call this unknown curve as g(X) curve. So, this g(X) curve is basically passing through 1, 0; 2, 2; and 3, 1. And now, if I apply the Lagrange's interpolation, I will get this. So, this will be my delta 1 polynomial; this will be my delta 2 polynomial; and this will be my delta 3 polynomial.

And now, remember, all the operations are performed over field. So, it should not interpret this as dividing by the denominator, but rather you should interpret it as multiplying with the multiplicative inverse. And I am denoting these values in colour because, these values are not available in clear, but parties have their shares of these coloured values; the uncoloured values, they are publicly known.

(Refer Slide Time: 47:33)



Linearity of Shamir Sharing: Example

- ❑ Ex: consider the field $(\mathbb{Z}_7, +_7, \cdot_7)$ --- addition/multiplication modulo 7
- ❑ $t = 1$, $n = 4$ and all instances of Shamir-sharing with $\alpha_1 = 1, \alpha_2 = 3, \alpha_3 = 4$ and $\alpha_4 = 5$

evaluation points
g(x)

	x		y		$\alpha_1 = 1$	$\alpha_2 = 3$	$\alpha_3 = 4$	$\alpha_4 = 5$	
x_1	1	y_1	0	$0 + 0 \cdot Z$	0	0	0	0	(4, 1)-Shamir SS of 0
x_2	2	y_2	2	$2 + 0 \cdot Z$	2	2	2	2	(4, 1)-Shamir SS of 2
x_3	3	y_3	1	$1 + 0 \cdot Z$	1	1	1	1	(4, 1)-Shamir SS of 1
x_{new}	0	y_{new}	?						

$(1,0), (2,2), (3,1)$

$\delta_1(x)$ $\delta_2(x)$ $\delta_3(x)$

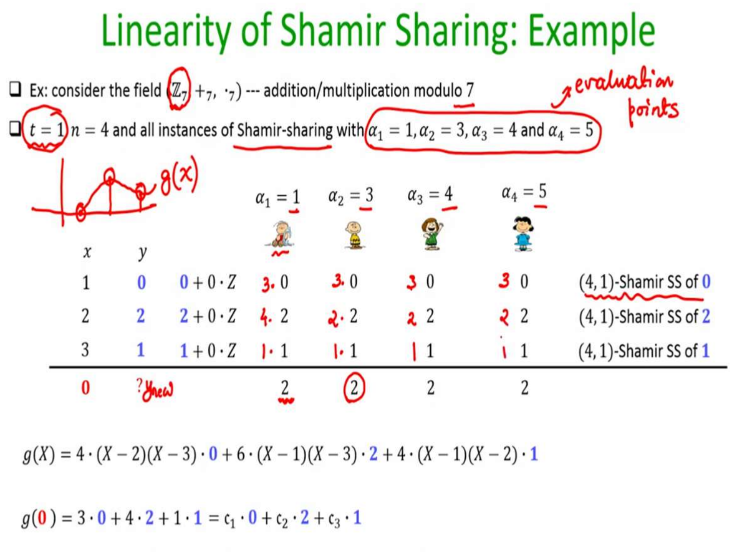
$$g(X) = \underbrace{4 \cdot (X-2)(X-3)}_{\delta_1(x)} \cdot 0 + \underbrace{6 \cdot (X-1)(X-3)}_{\delta_2(x)} \cdot 2 + \underbrace{4 \cdot (X-1)(X-2)}_{\delta_3(x)} \cdot 1$$

$$g(0) = \overset{c_1}{3} \cdot \overset{y_1}{0} + \overset{c_2}{4} \cdot \overset{y_2}{2} + \overset{c_3}{1} \cdot \overset{y_3}{1}$$

So, now if I simplify, I get that my unknown curve g(X) is this. That means, my goal is to compute g of 0; that is my x new. x new is 0, so, value of g 0 is nothing but, it is a linear combination of the existing y values. So, this is my y 1, y 2 and y 3. And these are my; so, this 3, 4, and 1, they constitute the Lagrange's coefficient. So, this is my Lagrange's coefficient c 1, Lagrange's coefficient c 2, Lagrange's coefficient c 3.

So, I obtain the fact that g of 0 is 3 * the first y value, 4 * the second y value, and 1 time the third y value; but the first y value, second y value and third y value, they are not available with any party, single party, but rather secret-shared.

(Refer Slide Time: 48:30)



Linearity of Shamir Sharing: Example

- ❑ Ex: consider the field $(\mathbb{Z}_7, +_7, \cdot_7)$ --- addition/multiplication modulo 7
- ❑ $t = 1$, $n = 4$ and all instances of Shamir-sharing with $\alpha_1 = 1, \alpha_2 = 3, \alpha_3 = 4$ and $\alpha_4 = 5$

evaluation points
g(x)

x	y		$\alpha_1 = 1$	$\alpha_2 = 3$	$\alpha_3 = 4$	$\alpha_4 = 5$	
1	0	$0 + 0 \cdot Z$	3 · 0	3 · 0	3 0	3 0	(4, 1)-Shamir SS of 0
2	2	$2 + 0 \cdot Z$	4 · 2	2 · 2	2 2	2 2	(4, 1)-Shamir SS of 2
3	1	$1 + 0 \cdot Z$	1 · 1	1 · 1	1 1	1 1	(4, 1)-Shamir SS of 1
0	? y_{new}		2	2	2	2	

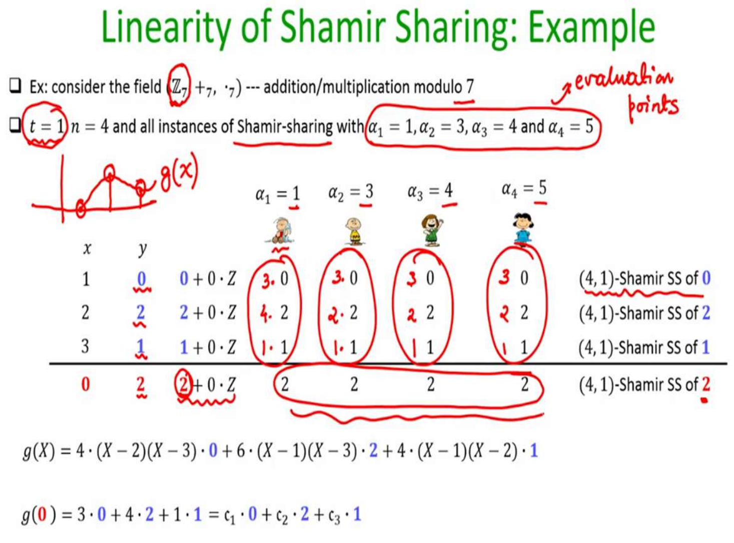
$$g(X) = 4 \cdot (X-2)(X-3) \cdot 0 + 6 \cdot (X-1)(X-3) \cdot 2 + 4 \cdot (X-1)(X-2) \cdot 1$$

$$g(0) = 3 \cdot 0 + 4 \cdot 2 + 1 \cdot 1 = c_1 \cdot 0 + c_2 \cdot 2 + c_3 \cdot 1$$

So, I have to just apply the same linear function individually on the shares of the respective parties. I means, I am asking the parties to do that. So, that means; now, what the first party will do? First party will take c_1; c_1 is 3, so, 3 * 0; c_2 is 4, so, 4 * 2; and c_3 is 1, so, 1 * 1. And all the operations are performed over the field. So, it is 4 * 2, 8; 8 + 1, 9; 9 modulo 7 is 2. So, this will be party 1's share of y new.

Same operation, party p 2 will do. c_1 * its share of first y value; 2 * its share of the second y value; and 1 * its share of the third y value; and it will obtain its share of the y new value. And like that, party 3 has to do; and similarly, party 4 has to do.

(Refer Slide Time: 49:41)



Linearity of Shamir Sharing: Example

- ❑ Ex: consider the field $(\mathbb{Z}_7, +_7, \cdot_7)$ --- addition/multiplication modulo 7
- ❑ $t = 1$, $n = 4$ and all instances of Shamir-sharing with $\alpha_1 = 1, \alpha_2 = 3, \alpha_3 = 4$ and $\alpha_4 = 5$

evaluation points
g(x)

x	y		$\alpha_1 = 1$	$\alpha_2 = 3$	$\alpha_3 = 4$	$\alpha_4 = 5$	
1	0	$0 + 0 \cdot Z$	3 · 0	3 · 0	3 0	3 0	(4, 1)-Shamir SS of 0
2	2	$2 + 0 \cdot Z$	4 · 2	2 · 2	2 2	2 2	(4, 1)-Shamir SS of 2
3	1	$1 + 0 \cdot Z$	1 · 1	1 · 1	1 1	1 1	(4, 1)-Shamir SS of 1
0	2	$2 + 0 \cdot Z$	2	2	2	2	(4, 1)-Shamir SS of 2

$$g(X) = 4 \cdot (X-2)(X-3) \cdot 0 + 6 \cdot (X-1)(X-3) \cdot 2 + 4 \cdot (X-1)(X-2) \cdot 1$$

$$g(0) = 3 \cdot 0 + 4 \cdot 2 + 1 \cdot 1 = c_1 \cdot 0 + c_2 \cdot 2 + c_3 \cdot 1$$

And now, you can see here clearly that these 4 values actually now constitute a vector of shares for the value 2, because they lie on this polynomial 2 + 0 Z, which is 1-degree polynomial whose constant term is 2; and this value 2 is basically the value of y new. That means, in this whole process, what I have demonstrated is, even without revealing the y_1, y_2 and y_3, the parties can apply, they can compute some linear operation on their respective shares of y_1, y_2, y_3, which will give them their respective shares of y new. With that, I end this lecture. Thank you.