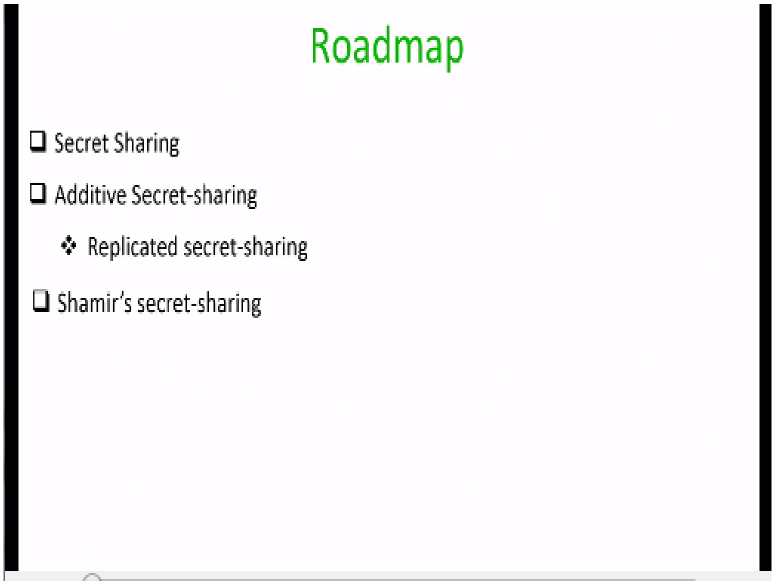
Foundations of Cryptography
Dr. Ashish Choudhury
Department of Computer Science
Indian Institute of Science – Bengaluru

Lecture - 56
Secret Sharing

(Refer Slide Time: 00:29)



Roadmap

- ❑ Secret Sharing
- ❑ Additive Secret-sharing
  - ❖ Replicated secret-sharing
- ❑ Shamir's secret-sharing

Hello everyone. Welcome to this lecture. So in this lecture we will discuss about interactive protocols. Namely our focus till now was on solving the problem of secure communication where we had two entities a sender and a receiver and we extensively discussed how to design algorithms to solve the problem of secure communication. But now what we are going to discuss is a scenario, a well-known problem, where we have multiple entities.

And our goal is to design cryptographic protocol which requires interaction among the entities. So, specifically the roadmap for this lecture is as follows. We will introduce the problem of secret sharing. We will see additive secret sharing, replicated secret sharing and then we will see the classic construction of secret sharing scheme due to Adi Shamir.

(Refer Slide Time: 01:17)

Secret Sharing : Motivation

❑ Access to the locker:

- ❖ Only if at least two managers come together and enter their password
- ❖ No access, if only a single manager enters its password

So let us see the motivation of secret sharing. So imagine we have a banking application, say where the locker in the bank is accessible only by the managers in the following way. The password for the locker is shared among the three managers and it shared in such a way that if only two of the managers go together and enter their respective passwords, the locker can be accessed.

But if only a single manager tries to enter the password and access the locker, the access is not possible. So, for instance if the second manager goes and tries to open the locker, it should not able to do that. In the same way, if the third manager goes alone, it should fail. But if we take any set of two or more number of managers and they go and enter their respective passwords, they should be able to access the locker. So that is what we require here.

(Refer Slide Time: 02:14)

Secret Sharing : Motivation

Access to Russia's Nuclear Weapons in 1990's

President

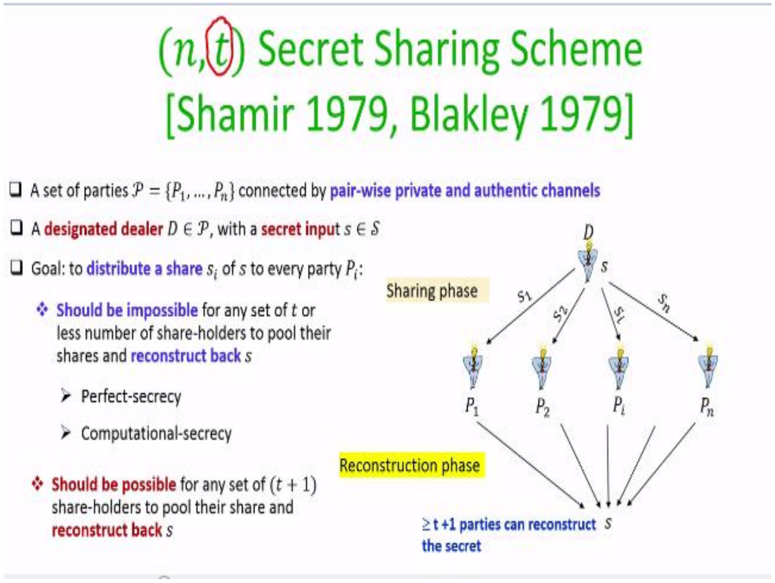
Prime Minister

Defence Minister

Nuclear Weapons could be accessed **ONLY IF AT LEAST TWO** of the above three entities come together

In the same way, consider another real-world scenario. This is a real-world scenario, which really happened during 90s. So this is regarding how Russia's Nuclear Weapons was accessible by the top leaders of the countries. So it is believed that the password to launch the Russia's nuclear weapon, it was shared between top three entities of the country namely the president, prime minister and defense minister in such a way that the weapon could be accessed or launched only if at least 2 of the 3 entities come together and enter their passwords, whereas if only a single entity tries to launch or access the weapon, the access will be denied.

(Refer Slide Time: 02:55)



(n,t) Secret Sharing Scheme [Shamir 1979, Blakley 1979]

❑ A set of parties $\mathcal{P} = \{P_1, \ldots, P_n\}$ connected by **pair-wise private and authentic channels**

❑ A **designated dealer** $D \in \mathcal{P}$, with a **secret input** $s \in \mathcal{S}$

❑ Goal: to **distribute a share** s_i of s to every party P_i:

- **Should be impossible** for any set of t or less number of share-holders to pool their shares and **reconstruct back** s
  - Perfect-secrecy
  - Computational-secrecy
- **Should be possible** for any set of $(t+1)$ share-holders to pool their share and **reconstruct back** s

Sharing phase

Reconstruction phase

$\geq$ t +1 parties can reconstruct s the secret

So both these applications can be abstracted by the following problem, which we call as (n, t) Secret Sharing. And this problem was independently formulated by Shamir in 1979 and Blakley in 1979. So what we are given here is, we are given the following setting. We have a set of n parties $P_1, \cdots P_n$ and they are connected by pair-wise private and authentic channel. What it means is, if any information P_i wants to send it to P_j, we assume that it has a dedicated channel with which it is connected to P_j. And anything P_i sends over that channel to P_j, it will be received correctly and securely by P_j. If you are wondering how exactly that such channels are available in real-world, well, we can use any of the well-known secure communication protocol that we have extensively discussed till now, to ensure that such channels are available between every pair of parties.

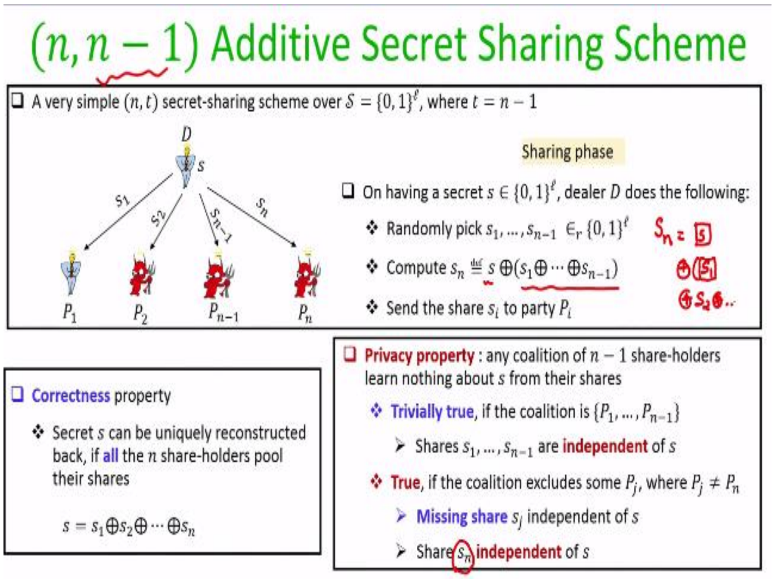
Now apart from these n parties, we have a designated party among those n parties and everyone will know the identity of that party and it is called as dealer. And dealer has some private input, a secret s from a bigger space $\mathcal{S}$, which is a set of all possible secrets. Now the goal of this dealer is to distribute its secret among the n parties by coming up or computing a share s_i for each of these parties and distributing the shares.

So first shareholder gets a share s_1, second party should get the second share and the party P_n should get the share s_n. And these shares are distributed over the pair-wise channel with which the dealer is connected to the individual shareholders. Now we require the following properties from these distributions of shares. We require that it should be impossible for any set of t or less number of shareholders to exchange their shares and reconstruct back the secret s.

And depending upon whether the set of t shareholders who are trying to reconstruct back the secret, whether they are computationally bounded or they are computationally unbounded, we achieve either perfect secrecy or computational secrecy. So that is the first requirement from this distribution of shares. On the other hand, if any set of $t + 1$ or more shareholders pull together their shares then it should possible to reconstruct back the secret s.

So the parameter t here is acting as a threshold for you. That means we require a sharing mechanism such that if any set of t or less number of shareholders come together, they should fail to access or they should fail to reconstruct the secret. The shares should be completely independent from the underlying secret. On the other hand, if any set of $t + 1$ or more number of shareholders come together, the secret should be reconstructed, it should be possible to reconstruct back the secret.

(Refer Slide Time: 05:39)



$(n, n-1)$ Additive Secret Sharing Scheme

❑ A very simple (n, t) secret-sharing scheme over $\mathcal{S} = \{0,1\}^\ell$, where $t = n - 1$

Sharing phase

❑ On having a secret $s \in \{0,1\}^\ell$, dealer D does the following:

❖ Randomly pick $s_1, \dots, s_{n-1} \in_r \{0,1\}^\ell$

❖ Compute $s_n \overset{\text{def}}{=} s \oplus (s_1 \oplus \cdots \oplus s_{n-1})$

❖ Send the share s_i to party P_i

❑ Correctness property

❖ Secret s can be uniquely reconstructed back, if all the n share-holders pool their shares

$$s = s_1 \oplus s_2 \oplus \cdots \oplus s_n$$

❑ Privacy property : any coalition of $n-1$ share-holders learn nothing about s from their shares

❖ Trivially true, if the coalition is $\{P_1, \dots, P_{n-1}\}$

- ➢ Shares $s_1, \dots, s_{n-1}$ are independent of s

❖ True, if the coalition excludes some P_j, where $P_j \neq P_n$

- ➢ Missing share s_j independent of s
- ➢ Share s_n independent of s

So let us see a very simple construction of $(n, n-1)$ additive secret sharing scheme. So basically here my threshold $t = n$. That means I require a sharing mechanism where all the n shareholders should come together to reconstruct back the secret. But if any single shareholder is missing then it should not be possible to reconstruct back the secret. And why it is called additive secret sharing, it would be clear to you very soon.

So here my secret space $\mathcal{S} = \{0,1\}^\ell$. The sharing algorithm is as follows. So imagine dealer has a secret $s \in \mathcal{S}$. To share it, it picks $n-1$ shares randomly from the set $\mathcal{S}$. That means the first share s_1 is a random ℓ-bit string, the second share is a random ℓ-bit string and in the same way the share s_{n-1} is also a random ℓ-bit string. Now once the first $n-1$ shares are fixed by the dealer, the last share s_n is set as $s_n = s \oplus s_1 \oplus \cdots \oplus s_{n-1}$. And once the n shares are computed, the dealers sends the respective shares to the respective shareholders. Namely the share s_i is given to the party P_i over the dedicated secure and authentic channel between the dealer and the party P_i.

So the correctness property here is trivial for this secret sharing, namely if all the n shareholders come together and exchange their shares with each other then indeed they can perform the xor of all the n shares and they will uniquely get back the underlying secret s which was shared by the dealer.

W next formally prove the privacy property here. So for privacy our goal is to show that if among these n shareholders, any $n-1$ shareholders come together and pull their shares, they should not learn anything about underlying secret s. So we divide the proof into two cases.

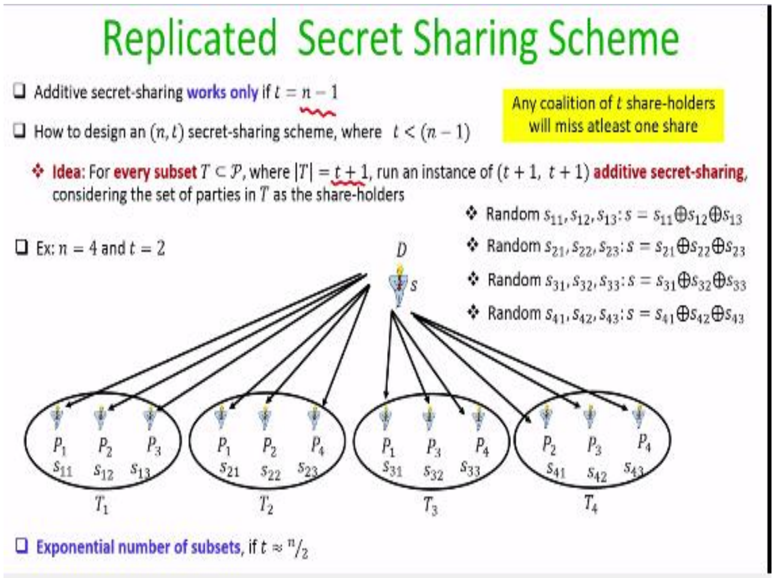
Consider the case when the set of $n-1$ shareholders who are corrupted and who are trying to reconstruct the secret are the first $n-1$ shareholders. It turns out that if the first $n-1$ shareholders are corrupt, then from their shares they learn absolutely nothing about underlying secret s. Because if you see the sharing algorithm, the first $n-1$ shares they are picked independently of the actual secret of the dealer. So that means if the adversary controls the first $n-1$ shareholders and access their shares, the adversary learns absolutely nothing about the dealer secret. That is the case one.

On the other hand, consider the case when the set of $n-1$ shareholders definitely include the nth shareholder, where the the share s_n is a function of a secret s and a remaining $n-1$ shares. So the second case is when coalition of $n-1$ shareholders excludes some party P_j, where P_j is definitely different from the party P_n.

So for simplicity you can imagine that my $P_j = P_1$, that means the adversary is corrupting the last $n-1$ shareholders here. It turns out that the missing share which the set of $n-1$ shareholders are missing, which in this example is the share s_1, that is independent of the secret s. Because that was picked randomly by the dealer and that ensures that even though the adversary learns s_n, it is the share s_n is also independent of the secret s. Because for instance, if we are considering the case where P_1 is missing in the coalition, then from the view part of the attacker, attacker knows that the value $s_n = s \oplus s_1 \oplus \cdots \oplus s_{n-1}$, where s and $s_1$are not known to the adversary. And where s_1 is independently and randomly picked by the dealer. So you can imagine that this s_n is nothing but a onetime pad encryption of the message s with a key, where the key is nothing but the xor of the shares $s_2, \cdots, s_{n-1}$which are known to the adversary and the random value s_1, which is not known to the attacker.

That means even though adversary is seeing s_n, it cannot figure out whether s_n is actually a share corresponding to the secret s or corresponding to a secret s'. Because it does not know the value of the missing share s_1, which was randomly picked and independently picked of the actual secret of the dealer. That ensures that even if the adversary controls the last shareholder it will learn absolutely nothing about the underlying secret s. And that is why the secret sharing satisfies the requirements of an $(n, n-1)$ secret sharing scheme.

(Refer Slide Time: 11:01)



Replicated Secret Sharing Scheme

- ❑ Additive secret-sharing **works only** if $t = n - 1$
- ❑ How to design an (n, t) secret-sharing scheme, where $t < (n - 1)$
  - ❖ **Idea:** For **every subset** $T \subset \mathcal{P}$, where $|T| = t + 1$, run an instance of $(t + 1,\ t + 1)$ **additive secret-sharing**, considering the set of parties in T as the share-holders

Any coalition of t share-holders will miss atleast one share

- ❑ Ex: $n = 4$ and $t = 2$

- ❖ Random s_{11}, s_{12}, s_{13}: $s = s_{11} \oplus s_{12} \oplus s_{13}$
- ❖ Random s_{21}, s_{22}, s_{23}: $s = s_{21} \oplus s_{22} \oplus s_{23}$
- ❖ Random s_{31}, s_{32}, s_{33}: $s = s_{31} \oplus s_{32} \oplus s_{33}$
- ❖ Random s_{41}, s_{42}, s_{43}: $s = s_{41} \oplus s_{42} \oplus s_{43}$

- ❑ **Exponential number of subsets**, if $t \approx {}^{n}/_{2}$

So it turns out that the additive secret sharing that we have discussed, it works only if my threshold is $n-1$. But in general I might be interested to design a secret sharing where my threshold may not be $n-1$, my threshold could be strictly less than $n-1$. So now let us see a solution, a naive solution of coming up with a secret sharing scheme for any threshold $t < n-1$.

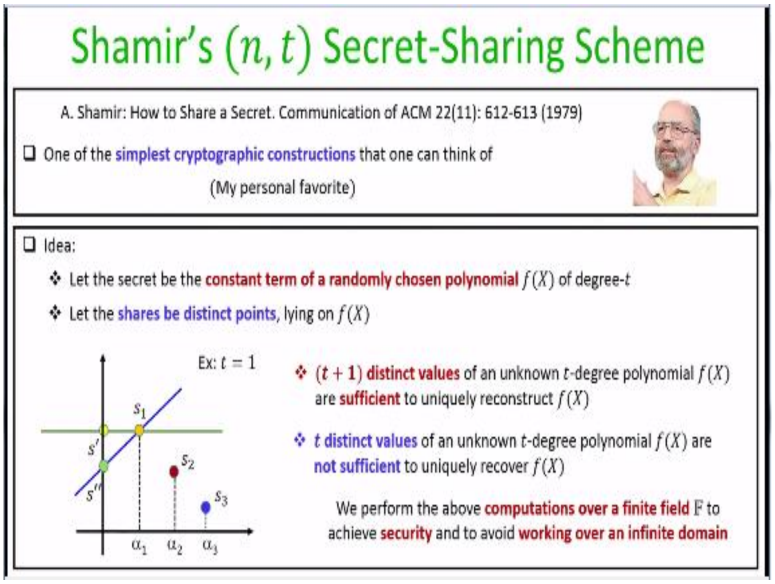
So the idea here is we take every proper subset of the set of the n parties, say T, where the size of T is $t+1$ and run a dedicated independent instance of additive secret sharing among the parties in T as the shareholders, with the threshold being $t+1$. And the idea here is that if we do this for every subset of size $t+1$, then when it comes to the actual coalition of t shareholders who might try to learn about the secret, that coalition of t shareholders will miss at least one share to reconstruct back the actual shared secret.

So what I am trying to say is best demonstrated by this example. So imagine my $n = 4$ and I want to design a scheme where my threshold $t = 2$. That means any subset of three shareholders should be able to reconstruct back the secret, but any set of two shareholders, if they try to pull their shares they should fail to reconstruct back the secret.

So the idea here is that the dealer divides this set of four parties into different subsets $T_1, T_2, T_{3,} T_4$ of size three parties. Now in the first subset $T_1 = \{P_{1,} P_2, P_3\}$, dealer runs an instance of additive secret sharing scheme with the threshold being t = 2. Namely dealer picks random shares $s_{11}, s_{12,} s_{13}$, such that $s = s_{11} \oplus s_{12} \oplus s_{13}$, and then the shares are given to the respective shareholder P_1, P_2, P_3. Similarly, the dealer runs an independent instance of (3, 3) additive sharing for the subset T_2, T_3 and T_4.

Now the overall share for P_1 will be all the shares which it receives in various instances of the (3, 3) additive sharing, depending upon the various subsets in which it is present. Namely its share will be s_{11}, s_{21} and s_{31}. Now it is easy to see that irrespective of which two parties get corrupt, because my threshold $t = 2$ in all the instances of additive sharing, those two shareholders learn absolutely no information about the secret s. So for instance if P_1 and P_2 gets corrupt, if they are under the control of the adversary then based on their shares that they learn, due to their presence in the subset T_1, the parties P_1, P_2 fail to learn the secret s, because they will be missing the share s_{13}. In the same way with respect to the subset T_2, these two parties will be missing the share s_{23} and that is why the secret s will not be known to them and so on. So it does not matter which subset of t parties get corrupt, based on their shares they fail to learn the actual secret . So now you might be wondering that we now have a secret sharing scheme for any threshold t with respect to the value of n. But it turns out that this scheme is inefficient because the number of subsets of size $t + 1$ is $\binom{n}{t+1}$, which becomes an exponential quantity if t is approximately $n/2$. That means dealers basically has to deal with exponential number of values here and same is the case for every shareholder. So this is an inefficient solution.

(Refer Slide Time: 15:53)



Shamir's (n, t) Secret-Sharing Scheme

A. Shamir: How to Share a Secret. Communication of ACM 22(11): 612-613 (1979)

❑ One of the **simplest cryptographic constructions** that one can think of

(My personal favorite)

❑ Idea:

- ❖ Let the secret be the **constant term of a randomly chosen polynomial** $f(X)$ of degree-t
- ❖ Let the **shares be distinct points**, lying on $f(X)$

- ❖ $(t+1)$ **distinct values** of an unknown t-degree polynomial $f(X)$ are **sufficient** to uniquely reconstruct $f(X)$
- ❖ t **distinct values** of an unknown t-degree polynomial $f(X)$ are **not sufficient** to uniquely recover $f(X)$

We perform the above **computations over a finite field** $\mathbb{F}$ to achieve **security** and to avoid **working over an infinite domain**

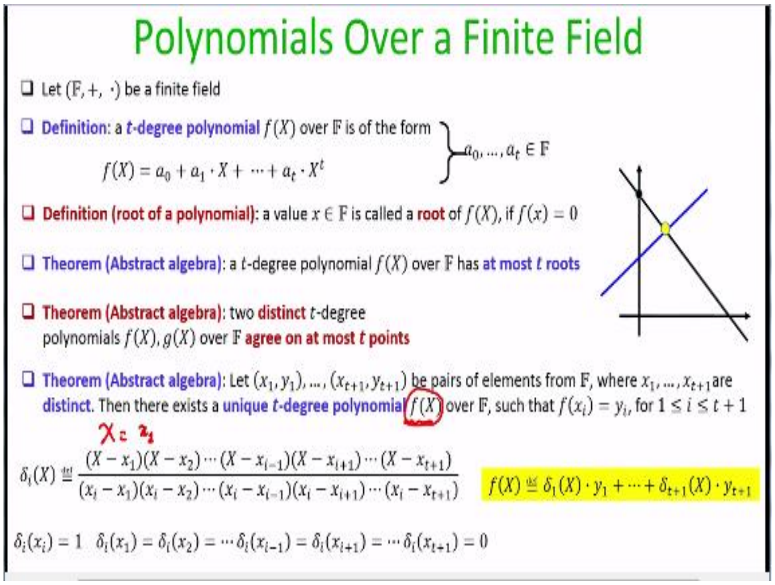
And let us know discuss a very clever solution for (n, t) Secret-Sharing due to Adi Shamir. And this is one of the simplest cryptographic constructions that you can think of. This is my personal favorite. And this is based on simple arithmetic which you might have learned during your high school. So the idea here is, if you want to share a secret s, then to share it you pick a random polynomial $f(x)$ of degree t, such that the constant term of the polynomial is the secret which you want to share. And let the shares be the distinct points or values lying on that polynomial.

To demonstrate my point, imagine my threshold $t = 1$ and I have a secret s and I am the dealer. What I can do is, to share the secret s, since my threshold $t = 1$, I pick a random straight line, it could be any straight line in the plane with the only restriction been that its constant term should be the secret s which I want to share. And what I now do is, I compute the value of the straight line at some fixed publicly known distinct values, say at $x = \alpha_1$, at $x = \alpha_2$ and at $x = \alpha_3$. And these are the shares for the first party, second party and third party respectively. It will be publicly known to everyone that the first party is obtaining the value of straight line the dealer has picked at $x = \alpha_1$ and so on.

So these α_i values, they are publicly known and everyone will know that α_i is associated with the party P_i. Now let us try to prove that why intuitively it satisfies the requirements of (n, t) secret sharing. So it is easy to see that if $t + 1$ shareholders come together then they can uniquely reconstruct back the t degree polynomial which dealer has picked. Because $t + 1$ distinct values on an unknown t degree polynomial suffice to uniquely reconstruct back that polynomial. So for example if $t = 1$ and say the first two shareholders come up with their shares s_1 and s_2, then they can uniquely find the straight line passing through the points (α_1, s_1) and (α_2, s_2) by fitting a straight line equation. Once they obtain the straight line, they can take the constant term of the straight line to be the recovered secret.

On the other hand, the second fact that we can use for polynomials of degree t is that, if you take any t shareholders who are the bad guys and they are trying to reconstruct back the dealer's secret, they will fail to do that. Because t distinct values does not suffice to uniquely recover back the unknown t degree polynomial $f(x)$ which was picked by the dealer. More specifically, in this example since $t = 1$, say the first shareholder is corrupt. Then from its viewpoint there could be infinite number of straight lines possible in the plane passing through the point (α_1, s_1) and hence infinite number of possible secrets. That means just based on t shares, adversary will completely fail to uniquely reconstruct back the dealer's original polynomial and hence the dealer's original secret s. That is the intuitive idea. It turns out that we have to perform all the above computations over some finite field to achieve security and to avoid working over an infinite domain.

(Refer Slide Time: 20:01)



Polynomials Over a Finite Field

- ❑ Let $(\mathbb{F}, +, \cdot)$ be a finite field
- ❑ **Definition:** a ***t*-degree polynomial** $f(X)$ over $\mathbb{F}$ is of the form $f(X) = a_0 + a_1 \cdot X + \cdots + a_t \cdot X^t$ } $a_0, \ldots, a_t \in \mathbb{F}$
- ❑ **Definition (root of a polynomial):** a value $x \in \mathbb{F}$ is called a **root** of $f(X)$, if $f(x) = 0$
- ❑ **Theorem (Abstract algebra):** a t-degree polynomial $f(X)$ over $\mathbb{F}$ has **at most *t* roots**
- ❑ **Theorem (Abstract algebra):** two **distinct** t-degree polynomials $f(X), g(X)$ over $\mathbb{F}$ **agree on at most *t* points**
- ❑ **Theorem (Abstract algebra):** Let $(x_1, y_1), \ldots, (x_{t+1}, y_{t+1})$ be pairs of elements from $\mathbb{F}$, where $x_1, \ldots, x_{t+1}$ are **distinct.** Then there exists a **unique *t*-degree polynomial** $\boxed{f(X)}$ over $\mathbb{F}$, such that $f(x_i) = y_i$, for $1 \leq i \leq t+1$

$X = x_1$

$$\delta_i(X) \overset{\text{def}}{=} \frac{(X - x_1)(X - x_2) \cdots (X - x_{i-1})(X - x_{i+1}) \cdots (X - x_{t+1})}{(x_i - x_1)(x_i - x_2) \cdots (x_i - x_{i-1})(x_i - x_{i+1}) \cdots (x_i - x_{t+1})}$$

$$f(X) \overset{\text{def}}{=} \delta_1(X) \cdot y_1 + \cdots + \delta_{t+1}(X) \cdot y_{t+1}$$

$$\delta_i(x_i) = 1 \quad \delta_i(x_1) = \delta_i(x_2) = \cdots \delta_i(x_{i-1}) = \delta_i(x_{i+1}) = \cdots \delta_i(x_{t+1}) = 0$$

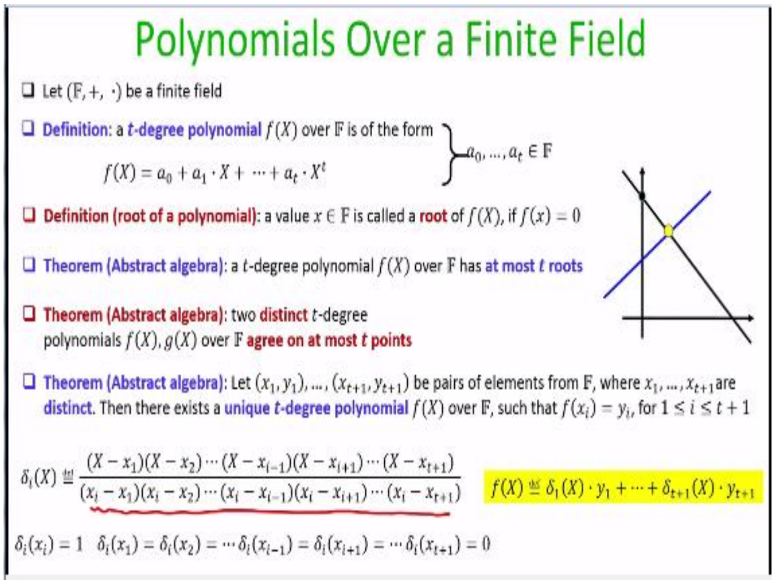
So let us try to first understand some basic facts about polynomials over a finite field. So imagine I am given a finite field $(\mathbb{F}, +, \cdot)$. A t degree polynomial $f(X)$ over $\mathbb{F}$ is of the form $f(X) = a_0 + a_1 \cdot X + \cdots + a_t \cdot X^t$, where $a_0, \ldots, a_t \in \mathbb{F}$. A value $x \in \mathbb{F}$ is called a root of $f(X)$, if $f(x)$ =0

I stress here that all the operations here are the $+$ and $\cdot$ operations over the field. Now another well-known fact from abstract algebra which we can use here is the following. If you are given a t degree polynomial over a field, then it can have at most t roots. For example, if $t = 1$, then a straight over a field meets the y-axis at atmost one point. And this is true for any t degree polynomial over a field. And based on this result, we can state that two distinct t-degree polynomials $f(X)$, $g(X)$ over $\mathbb{F}$ can have at most t common values. So for instance if you have 2 distinct straight lines they can intersect at atmost one point. They cannot intersect at 2 points because if they intersect at two common points then the 2 straight lines are basically the same straight line and in general, this generalizes for any value of t.

Again I am not proving this theorem. These are some well-known results from abstract algebra. And the final result which I am going to use for giving the description of Shamir's sharing is the Lagrange interpolation formula. So what this theorem basically says is if you are given t + 1 pairs of values (x_1, y_1), ..., (x_{t+1}, y_{t+1}) from the field, where $x_1, \ldots, x_{t+1}$ are distinct. Then there exists a unique t-degree polynomial $f(X)$ over $\mathbb{F}$, such that $f(x_i) = y_i$, for $1 \leq i \leq t + 1$

To see how exactly we can compute this polynomial $f(X)$, let me define a sequence of $t + 1$ polynomials, where the i^{th} polynomial $\delta_i(X) \overset{\text{def}}{=} \frac{(X-x_1)(X-x_2)\cdots(X-x_{i-1})(X-x_{i+1})\cdots(X-x_{t+1})}{(x_i-x_1)(x_i-x_2)\cdots(x_i-x_{i-1})(x_i-x_{i+1})\cdots(x_i-x_{t+1})}$, which has degree t. And the way I have defined this polynomial $\delta_i(X)$, it follows that $\delta_i(x_i) = 1$, while $\delta_i(x_1) = \delta_i(x_2) = \cdots \delta_i(x_{i-1}) = \delta_i(x_{i+1}) = \cdots \delta_i(x_{t+1}) = 0$. That means these $\delta_i(X)$ polynomials are such that they survive at $X = x_i$, whereas they vanish at all other x_i values. Now my unknown polynomial passing through the t + 1 given pairs of (xi, yi) values. And I can represent that unknown polynomial $f(X) = \delta_1(X) \cdot y_1 + \cdots + \delta_{t+1}(X) \cdot y_{t+1}$.

(Refer Slide Time: 24:43)



Polynomials Over a Finite Field

- ❑ Let $(\mathbb{F}, +, \cdot)$ be a finite field
- ❑ **Definition:** a ***t*-degree polynomial** $f(X)$ over $\mathbb{F}$ is of the form $f(X) = a_0 + a_1 \cdot X + \cdots + a_t \cdot X^t$ $\Big\}$ $a_0, \ldots, a_t \in \mathbb{F}$
- ❑ **Definition (root of a polynomial):** a value $x \in \mathbb{F}$ is called a **root** of $f(X)$, if $f(x) = 0$
- ❑ **Theorem (Abstract algebra):** a t-degree polynomial $f(X)$ over $\mathbb{F}$ has **at most *t* roots**
- ❑ **Theorem (Abstract algebra):** two **distinct** t-degree polynomials $f(X), g(X)$ over $\mathbb{F}$ **agree on at most *t* points**
- ❑ **Theorem (Abstract algebra):** Let $(x_1, y_1), \ldots, (x_{t+1}, y_{t+1})$ be pairs of elements from $\mathbb{F}$, where $x_1, \ldots, x_{t+1}$are **distinct**. Then there exists a **unique *t*-degree polynomial** $f(X)$ over $\mathbb{F}$, such that $f(x_i) = y_i$, for $1 \leq i \leq t+1$

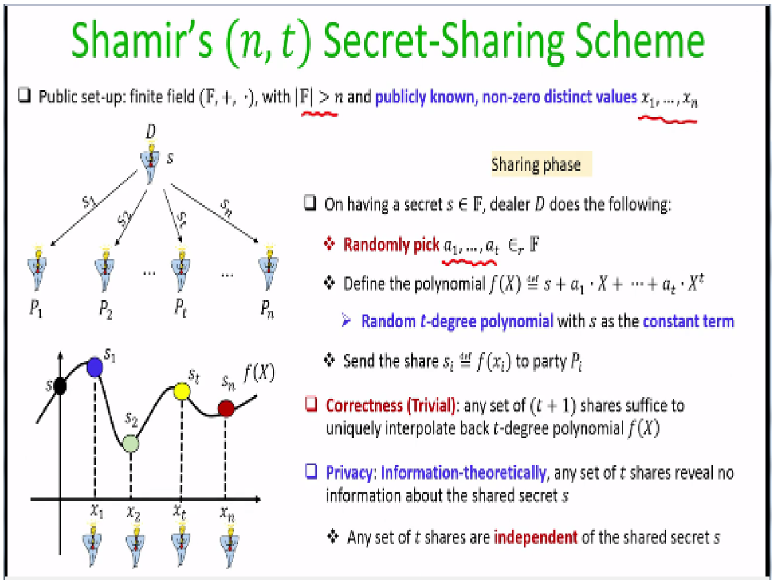
$$\delta_i(X) \overset{\text{def}}{=} \frac{(X - x_1)(X - x_2) \cdots (X - x_{i-1})(X - x_{i+1}) \cdots (X - x_{t+1})}{(x_i - x_1)(x_i - x_2) \cdots (x_i - x_{i-1})(x_i - x_{i+1}) \cdots (x_i - x_{t+1})} \qquad f(X) \overset{\text{def}}{=} \delta_1(X) \cdot y_1 + \cdots + \delta_{t+1}(X) \cdot y_{t+1}$$

$$\delta_i(x_i) = 1 \quad \delta_i(x_1) = \delta_i(x_2) = \cdots \delta_i(x_{i-1}) = \delta_i(x_{i+1}) = \cdots \delta_i(x_{t+1}) = 0$$

And it is easy to see that indeed $f(x_1) = y_1$, because for $X = x_1$, my $\delta_1(X)$ polynomial will survive and give the value 1 and 1 multiplied by y_1 will be y_1, whereas all the other $\delta_i(X)$ polynomials will vanish off. In the same way for $X = x_2$, all my delta polynomials will vanish except the $\delta_2(X)$ polynomial, which will give the value 1 and 1 multiplied by y_2 will give me y_2, which satisfies my condition.

So that is the unique t degree polynomial $f(X)$, which you can find out passing through the given points (x_1, y_1), ..., (x_{t+1}, y_{t+1}), where $x_1, \ldots, x_{t+1}$ are distinct. Now you might be wondering that why $x_1, \ldots, x_{t+1}$ are distinct have to be distinct? They have to be distinct to ensure that each of the $\delta_i(X)$ polynomials have a denominator which is non-zero. And if denominator is non-zero then basically this numerator divided by denominator should be interpreted as if this numerator is multiplied by the multiplicative inverse of my denominator, because I am doing the division here. And this division should be interpreted as multiplying the numerator with the multiplicative inverse of the denominator. And the multiplicative inverse of the denominator will exist only if my denominator is non-zero.

(Refer Slide Time: 26:08)



Shamir's (n, t) Secret-Sharing Scheme

- ❑ Public set-up: finite field $(\mathbb{F}, +, \cdot)$, with $|\mathbb{F}| > n$ and publicly known, non-zero distinct values $x_1, \dots, x_n$

Sharing phase

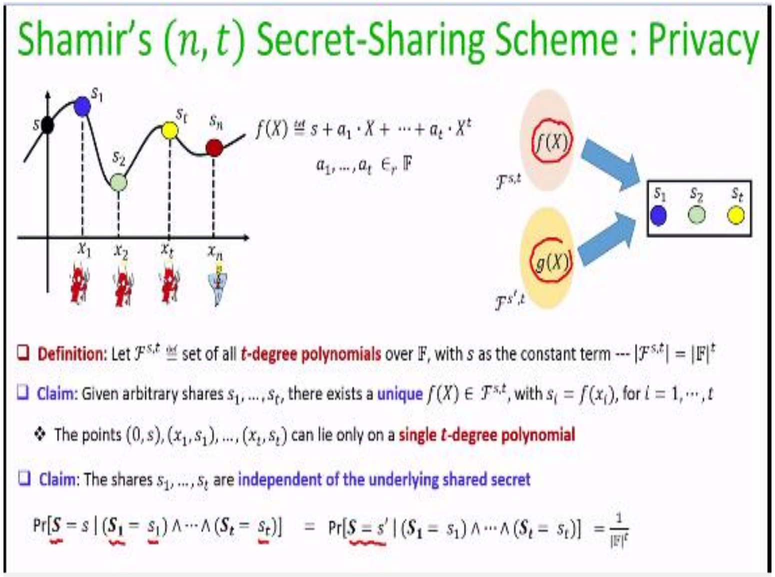
- ❑ On having a secret $s \in \mathbb{F}$, dealer D does the following:
  - ❖ Randomly pick $a_1, \dots, a_t \in_r \mathbb{F}$
  - ❖ Define the polynomial $f(X) \overset{\text{def}}{=} s + a_1 \cdot X + \dots + a_t \cdot X^t$
    - ➢ Random t-degree polynomial with s as the constant term
  - ❖ Send the share $s_i \overset{\text{def}}{=} f(x_i)$ to party P_i
- ❑ Correctness (Trivial): any set of $(t + 1)$ shares suffice to uniquely interpolate back t-degree polynomial $f(X)$
- ❑ Privacy: Information-theoretically, any set of t shares reveal no information about the shared secret s
  - ❖ Any set of t shares are independent of the shared secret s

So now let us go to the description of Shamir's Secret Sharing. As part of public setup, we will be given some finite field where the size of the field will be at least n, the number of shareholders. And associated with the shareholders will be n publicly known non-zero distinct values, namely $x_1, \dots, x_n$, which are the values from the finite field. The sharing algorithm of Shamir secret sharing is as follows. If the dealer has a secret value s, which he wants to share then it picks a random polynomial $f(X)$ over the field by choosing t random elements as the coefficients from the field, such that the constant term of the polynomial $f(X)$ is the secret s which dealer wants to share. And now the i^{th} shareholder, namely the party P_i, gets the share s_i, where s_i is nothing but the value of this polynomial picked by the dealer at $X = x_i$.

The correctness of this secret sharing is trivial. That means, imagine out of these n shareholders, any subset of $t + 1$ shareholders come together by exchanging their shares, then they can uniquely interpolate back the t degree polynomial $f(X)$ using the Lagrange's interpolation formula that we have discussed earlier.

And to prove the privacy we are going to prove that if we take any set of t shareholders among these n shareholders, then their shares are independent of the underlying share secret s, because intuitively this comes from the fact that the coefficients of polynomial which are picked by dealer for sharing the secret, are chosen uniformly at random from the underlying field.

(Refer Slide Time: 27:55)



Shamir's (n, t) Secret-Sharing Scheme : Privacy

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

$a_1, \ldots, a_t \in_r \mathbb{F}$

❑ **Definition:** Let $\mathcal{F}^{s,t} \overset{\text{def}}{=}$ set of all ***t*-degree polynomials** over $\mathbb{F}$, with s as the constant term --- $|\mathcal{F}^{s,t}| = |\mathbb{F}|^t$

❑ **Claim:** Given arbitrary shares $s_1, \ldots, s_t$, there exists a **unique** $f(X) \in \mathcal{F}^{s,t}$, with $s_i = f(x_i)$, for $i = 1, \cdots, t$

❖ The points $(0, s), (x_1, s_1), \ldots, (x_t, s_t)$ can lie only on a **single *t*-degree polynomial**

❑ **Claim:** The shares $s_1, \ldots, s_t$ are **independent of the underlying shared secret**

$\Pr[\underset{\sim}{S} = s \mid (\underset{\sim}{S_1} = \underset{\sim}{s_1}) \wedge \cdots \wedge (S_t = \underset{\sim}{s_t})] = \Pr[\underset{\sim}{S = s'} \mid (S_1 = s_1) \wedge \cdots \wedge (S_t = s_t)] = \frac{1}{|\mathbb{F}|^t}$

So let us make it more rigorous. So let me define a set $\mathcal{F}^{s,t}$ to denote the set of all t-degree polynomials selected from the finite field whose constant term is the secret s. So it turns out that the number of such polynomial of degree t whose constant term is the secret s is nothing, but $|\mathbb{F}|^t$. This is because in every such polynomial, apart from the constant term which is s, there are t other coefficients $a_1, \cdots, a_t$ picked from the field and for each of these coefficients, there are $|\mathbb{F}|$ candidates. Hence $|\mathcal{F}^{s,t}| = |\mathbb{F}|^t$.

For simplicity and without loss of geniality, assume that first t shareholders are corrupt, that means they have seen the shares $s_1, \ldots, s_t$. And they know that these shares are nothing but the value of some unknown t degree polynomial $f(X)$, evaluated at $X = x_1, \ldots, x_t$. We will show that the probability distribution of these t shares is independent of the secret picked by the dealer. For this, we first note that given any arbitrary shares $s_1, \ldots, s_t$, there exists a unique polynomial $f(X) \in \mathcal{F}^{s,t}$, with $s_i = f(x_i)$, for $i = 1, \cdots, t$. This follows from the fact that the $t + 1$ distinct points (0, s), (x_1, s_1), …, (x_t, s_t) can lie only on a single t -degree polynomial.

Now based on all these things, I claim that the shares $s_1, \ldots, s_t$ are independent of the actual secret shared by the dealer. And to prove this claim, let us consider a pair of arbitrary secrets (s, s') from $\mathbb{F}$, such that $s \neq s'$. We will show that from the view point of the adversary, $s_1, \ldots, s_t$ could be the shares of s as well as s' with equal probability. Let $f^s(X)$ be unique polynomial from the set $\mathcal{F}^{s,t}$ which would have produced the shares $s_1, \ldots, s_t$ for the secret s. And similarly, let $f^{s'}(X)$ be the unique polynomials from the set $\mathcal{F}^{s',t}$, which would have produced the shares $s_1, \ldots, s_t$ for the secret s'. Now the probability that given adversary has seen the shares $s_1, \ldots, s_t$, dealer's secret is s is the same as dealer has used the polynomial $f^{s}(X)$ for sharing. And this event occurs with probability $1/|\mathbb{F}|^t$, as dealer's polynomial is randomly picked over $\mathbb{F}$, where all the coefficients except the constant term are randomly selected from $\mathbb{F}$. Using exactly the same argument, we conclude that the probability that given adversary has seen the shares $s_1, \ldots, s_t$, dealer's secret is s' is the same as dealer has used the polynomial $f^{s'}(X)$ for sharing. And this event occurs with probability $1/|\mathbb{F}|^t$. That proves that the probability distribution of $s_1, \ldots, s_t$ is independent of the underlying secret and hence on seeing these shares, adversary will be clueless whether dealer has shared the secret s or secret s'.

So that brings me to the end of this lecture. Just to summarize. In this lecture we introduced the problem of (n, t) secret sharing and we saw three constructions. We saw the construction of additive secret sharing where the threshold is $n - 1$. And then using this $(n, n - 1)$ secret sharing exponential number of times, we saw a solution for any (n, t) secret sharing which we call as replicated secret sharing. And finally we saw a clever construction of (n, t) secret sharing which is a poly time solution for any value of n and t due to Shamir.