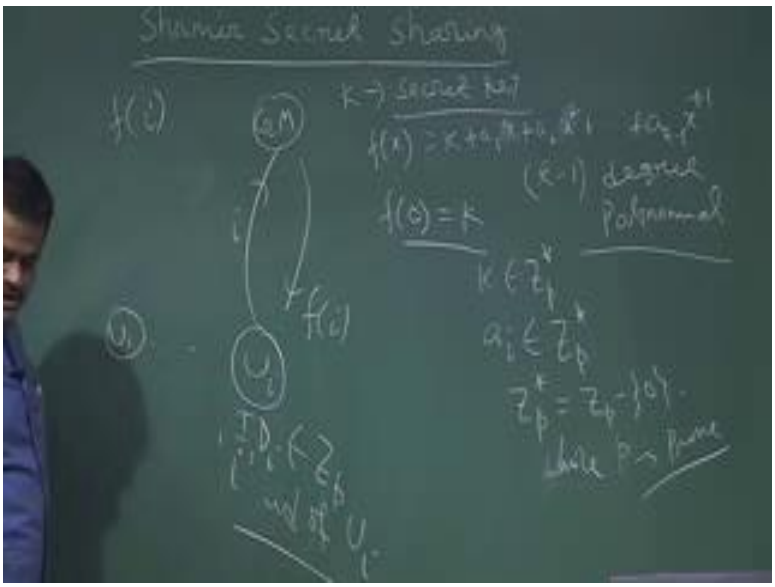
Internetwork Security
Prof. Sourav Mukhopadhyay
Department of Mathematics
Indian Institute of Technology, Kharagpur

Lecture – 53
Shamir Secret Sharing

(Refer Slide Time: 00:29)



So, we talk about secret sharing - Shamir secret sharing which is basically a t n threshold secret sharing scheme t n threshold secret sharing scheme by Shamir. So, basically there are n users or n participants, and there is a group manager. So, there is a group manager or the leader dealer or something and there are n users, so u 1, u 2, u n. And now there is a secret key or the session key because this needs to change by session wise.

Suppose, this is a for example, suppose this is a TV channel operator, cable operator - Tata sky or some cable service provider, and these are the users who subscribe for this channel. So, now this cable operator will broadcast something some movie or something, so that is the movie or something, so that movie need to be encrypt using a key. So, that key is a session key because it has to change because some user may get revoked if I am not paying the subscription I will be in the revoked list of this thing. So, this k is the session key.

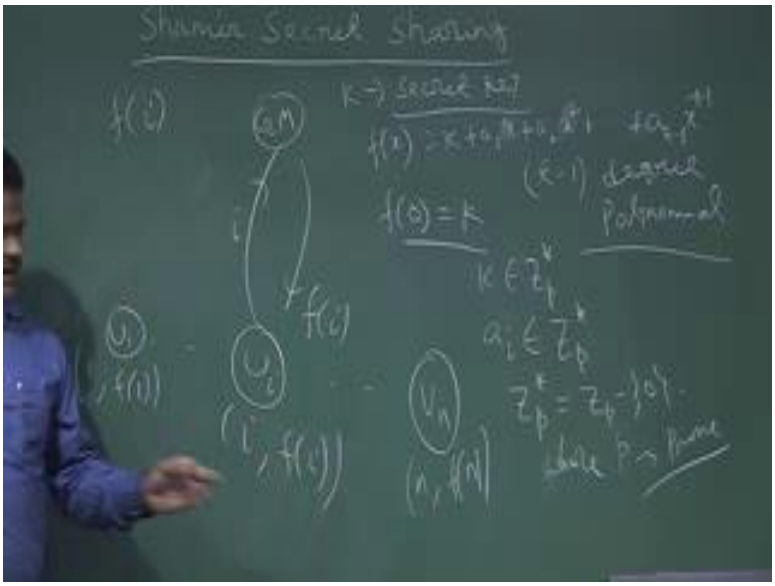
So, now, this question is how we can share this key among the users, so that when the t user when users, so that k be the key this is the secret key. So, the question is how we

can share some information with this user, so that when t user come together then they should able to recover the key, so that is called t n threshold scheme, t n threshold secret sharing scheme. So, there are n users. If the t user come together then they should able to recover this secret key.

So, what is the scheme? So, scheme is basically, so group manager or the dealer will choose the polynomial f x of the degree t minus 1. So, just like this a 1 t and putting this f 0 as k. So, a 1 t, a 2 t square sorry a 1 x, a 2 x square plus a t minus 1 to the power t minus 1, so t minus 1 degree polynomial. So, the group manager or the dealer will chose a t minus 1 degree polynomial, and put this k as a constant, so that means, f 0 is basically the secret or the secret key which we are going to shared among the n users, so that if t users come together, they should able to recover this secret.

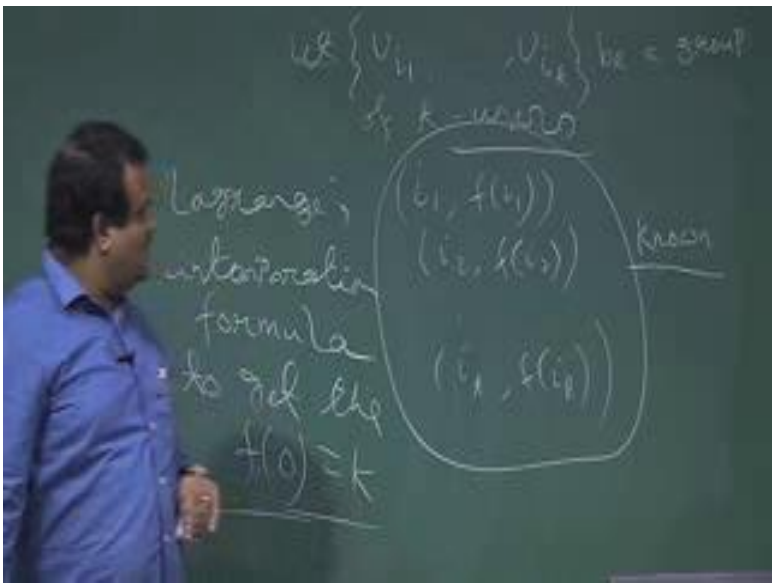
So, how we can do that? So, this is a t minus 1 degree polynomial. So, there are how many constant, there are basically t constant. So, now, suppose these are the users u 1, u i. So, group manager will give some secret to the u i, secret or the share of u i. So, what will be the share of u i. So, either u i and this a i's are coming from this key is basically Z p star and this ai's are also we are taking from Z p star or p is a prime. So, Z p star is basically Z p minus 0, where p is a prime. So, Z p star is a cyclic group under the multiplicative operation; p is prime. So, it is ith user either we chose a ID of this. So, ID also should be belongs to Z p star or we can convert into some we can use some mapping or we can simply use i. So, this is the say i is the ID for simplicity we take this i is the ID of u i for simplicity, but it could be anything I mean it could be any ID and then we have to convert into 0, 1 string or in a element in Z p star. So, then this will send the ID to G m. So, while G m will do, G m has the polynomial, G m has chosen the polynomial. So, G m will compute this f of i and send this f of i to in a secured way. So, this is the shared of this.

(Refer Slide Time: 06:45)



So, u i has this share i, f of i or it could be if x i is the ID x i f of x i in general, but for the simplicity we can take the i, f of i . So, this everybody has so this is 1 f of 1 for user 1, 2 f of 2, so similarly u n has n f of n. So, now this is the share where share is basically a point and the value of the polynomial at that point; and that point is basically their ID or they could choose any point or by their own. So, now how they can now compute k, so now, this is the polynomial of degree t minus 1. Now, suppose t users come together with their shares. So, these are their share.

(Refer Slide Time: 07:57)



Now, t users come together like u i 1, u i t, let this be a group of t users. This is t n session scheme. So, if a group of t user comes together, they should able to get the secret. So, this is the aim of this t n threshold secret sharing scheme. So, now if they come together how they can get the key, this means they have they know the value f of i 1, i 2, f of i 2, i t, f of i t, so these values are known. So, we have a polynomial of degree t where there are degree t minus 1, but there are t many unknown constant. So, now we can use some interpretation formula like we can use the Lagrangian interpolation formula, because these points are not equidistance. So, Newton will may not work here, because these points are basically their id's. So, we do not know which groups of users are coming together. So, they are not equidistance.

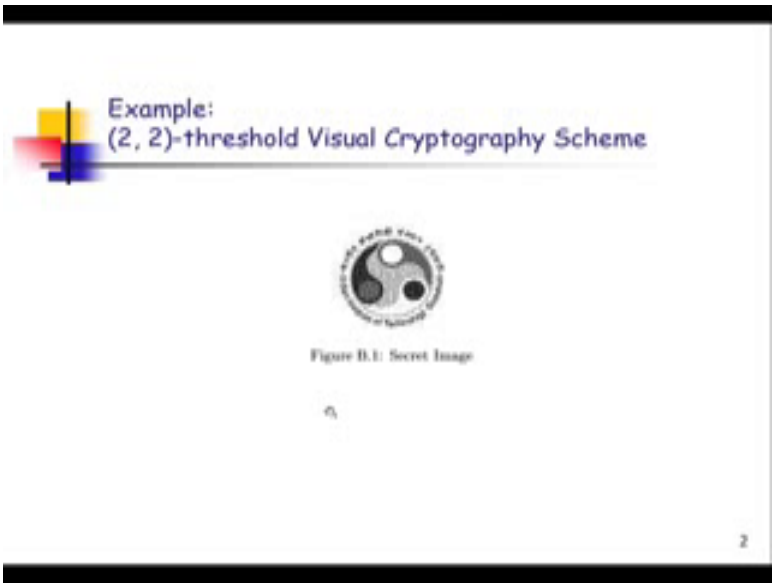
So, one can use the Lagrange interpolation formula to find out to get the whole polynomial, Lagrange's interpolation formula to get the polynomial or f of g polynomial values at 0, to get f of 0. So, this is basically k, so k is revealed. So, if the t users come together with their polynomial value at their points then we can solve the, we can use the Lagrange interpolation formula to know the whole polynomial. So, whole polynomial is revealed. So, this is the basically so many t n threshold secret sharing scheme. So, it has application in visual cryptograph and broadcast encryption.

(Refer Slide Time: 10:55)

So, in visual cryptograph, can you go to the slid please? So, this is basically k n threshold scheme where a secret s is divided into n pieces. Suppose, this could be application in

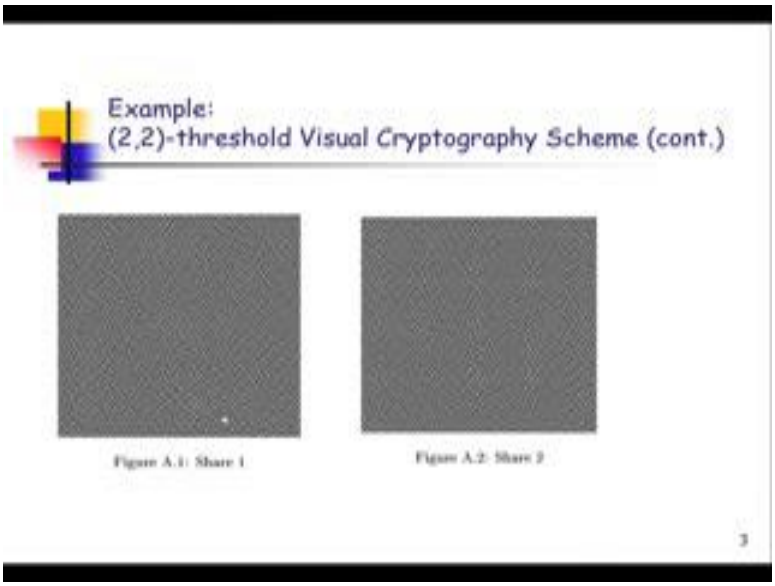
banking system suppose we have a locker. So, you know locker in the bank, locker a key is with the group, bank manager and a key is with the user. So, when they together meet, they should able to open the locker, so that is the secret sharing. So, locker key is the secret. So, we are sharing into we are giving the share to the bank manager and the users. So, when they come together, they only able to open the locker. So, here this is a k n threshold scheme. So, you are divided the secret s into n pieces such that if the k users or more come together, they should able to recover the secret, but if there are k minus 1 or less users are coming then they should not able to recover the secret.

(Refer Slide Time: 11:57)



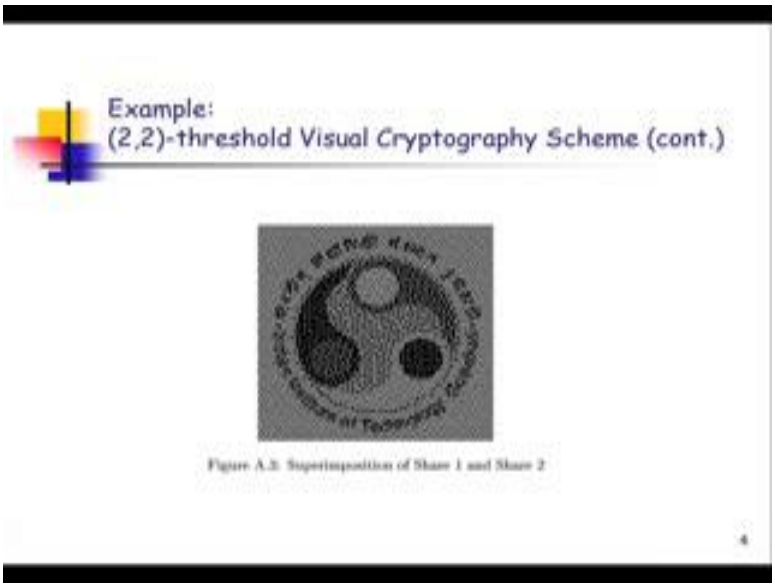
So, this is an simple example of two threshold scheme suppose this is the secret image and we want to share between two users; and when the two user will be coming together then they should able to. So, this is the secret image.

(Refer Slide Time: 12:14)



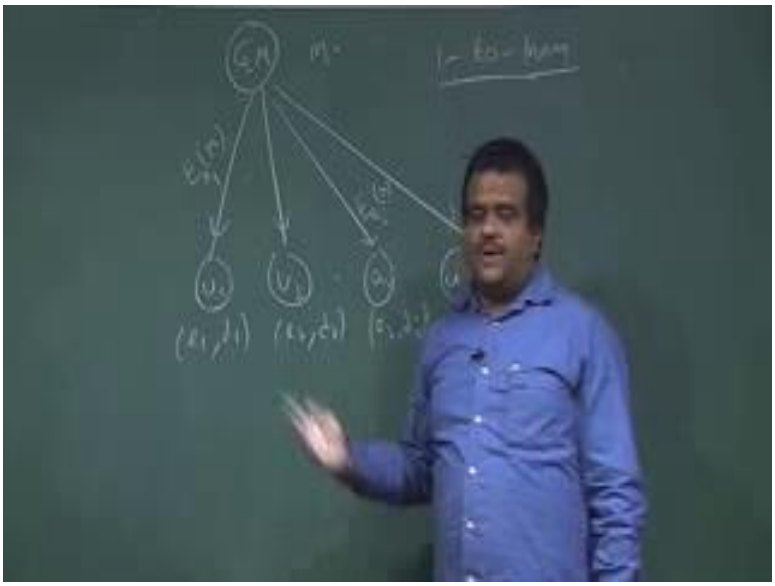
So, this is that the share for two users - share 1, share 2. So, now, by seeing this picture nobody can guess that was the symbol of IIT, logo of IIT, Guwahati. Now, this is also this thing.

(Refer Slide Time: 12:38)



Now, but if they come together if you just merge this two then this will be like this, superimposition this share one and share two like this. So, then it will be a then it will reveal the secret. So, this has application in visual cryptography. Now, we will talk about some application in like broadcast encryption for Shamir secret sharing scheme.

(Refer Slide Time: 13:10)



So, in broadcast encryption, we have a group manager. A broadcast encryption is basically 1-to-many. So, for our encryption, I mean in public key, suppose we have many users like u 1, u 2 we have many users u 1, u 2, u a, and suppose we have a group manager, and group manager wants to send some message to this users. Now, so far we know 1-to-1 encryption that means, everybody is having their private key and the public key pair, so e 1, d 1; e 2, d 2; e n, d n.

Now if some message has to send to u 1. So, what we do we just this is the general public key setup in the normal public key 1-to-1 public key encryption what we do we suppose this is the message. So, we just encrypt this to send u 1, we will just encrypt this message using the public key of u 1. So, it is basically encryption of M u 1, and similarly this, this. So, for u i, it is basically e ID i is the corresponding public key private key pair. So, this is basically encryption of e i M, so that means this Ciphertext size is very big. So, these, these, these all this has to combine and moreover this is one has to get their corresponding Ciphertext that is this is a huge bottom neck of this. So, instead of that this is 1-to-1 corresponding. So, in broadcast encryption, what we will do we do one to many, and to send the Ciphertext, broadcast the Ciphertext in a single go and then the person, legitimate users should be able to decrypt it.

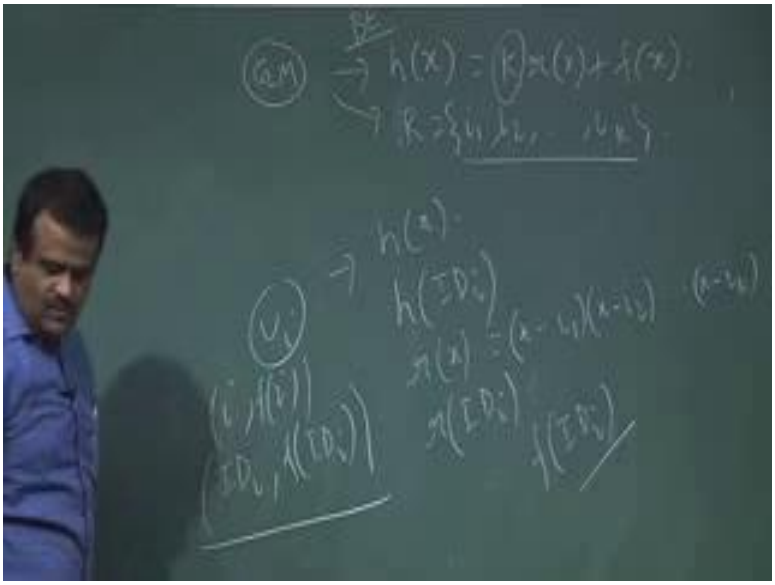
(Refer Slide Time: 15:46)

So, how we can use this Shamir secret sharing scheme for this purpose. So, let us just so this is group manager and these are the users u 1, u 2, u i, u n. And suppose this is the secret key group manager wants to share to these users. So, that and this is the set of revoked users set revoked user set say R, so u i 1, u i 2, u i 3 suppose these are this is the set of revoked users. So, revoked user now we want to send the message, broadcast the Ciphertext in such a way such that revoked users should not get the information. What is the key, now this is suppose the session key for time being. Now this session key we want to share between this, so that revoked users should not get the session key, because this session key is we used to encrypt the movie, if it is like cable line operator this G m. So, this will be used to encrypt the movie. So, if the revoked user that means, who did not pay for the movie or unsubscribed from this channel. So, he or she should not able to get this movie.

So, what we will do, we just group manager will compute a polynomial like this. First compute a revoked polynomial which is r x is basically by taking the indexes of x minus i k and compute f of x. F of x is a t minus 1 degree polynomial so that means, f of x is some a 0 plus a 1 x plus a t x to the power t minus 1 t minus 1 to the polynomial. So, this is also t n threshold scheme we are discussing, but in a broadcast encryption, so there are revoked users. So, we do not want to revoked we are not allowing revoked user to get some information. So, what we will do? We just, so then G m will compute this; this is

the session key k and masking with the revoked user polynomial plus f of x. So, this is the polynomial. So, this is the polynomial it is calculating.

(Refer Slide Time: 19:43)

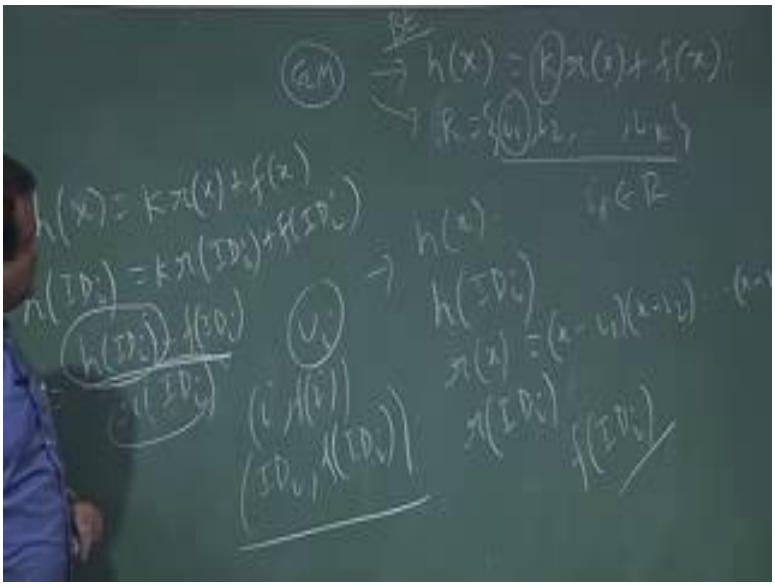


Now, so gm is calculating this polynomial h of x, and this is also a t degree polynomial. So, h of x is computing now suppose a user is joining in the initially. So, f of x is also with the, so both are trading with the polynomial. So, this is the u i users. So, what u i is having what g m is giving to u i at the time of registration, it is giving us f of u i, so f of i basically. So, this value it is having so identity. I mean or ID of i f of ID of i. So, this value it is having. So, this value it is having.

So, now, what G M is doing? So, G M is broadcasting this h of x. So, G M is broadcasting this h of x, h of x is basically k of r of x plus f of x. So, now, this users is getting h of x, now after getting h of x is what this user can do user need to get the session key k. So, user can compute h of ID because h of x means the polynomial whole polynomial G M is broadcasting. So, it is a t degree polynomial. So, basically it is broadcasting the t points on this polynomial. So, anybody can do the interpolation using the Lagrange to get the l polynomial. So, anyway, so this person u i is can calculate this. So, after calculating this is what and also it is broadcasting the revoked user set. So, what are the things it is broadcasting this polynomial along with the r r is the revoked user in this sets.

So, from here this user u i can compute r of x, r of x is basically x minus i 1 x minus i 2 x minus i 3. So, basically it can compute r of ID of this. So, once it this has this, and it has f of ID of i because this is the secret which is already it is having. So, it can simply now compute.

(Refer Slide Time: 22:48)



So, we know the h of x is basically k r of x plus f of x. So, h of ID i or it could be just i to simplicity, but ID should be element for Z p star anyway, so K r at ID i plus f of ID i. So, from here K is basically h of ID i minus f of ID i by divided by r of ID i. So, this is basically now this value user is computing by because this value this polynomial is broadcasted by the group managers. So, this value can be computed by the user and this value it is having, and this value can also can be computed by the user because his ID is not belongs to the revoked list. So, these values also can be computed by the users.

So, by doing this calculation user can get the session key k, but the problem will be the revoked users. Because for revoked user they will try to put their value over here with their ID their own ID is basically either of this suppose a user say k i, k i is the revoked user sorry i 1 is a revoked user. So, if we try to get this value, then this part will be 0, because this will be 0 for any value for revoked user value this will be 0. So, this will not give us the corresponding secret key because of this revoked view. Now, this scheme we can make it to the t n threshold scheme, because this polynomial if we know this

polynomial f say suppose yeah, so if somebody knows this polynomial f completely then he or she can able to get the session key.

(Refer Slide Time: 25:21)

Because we know the h of x is basically k r of x plus f of x. Now, if we can calculate some value j say h of say x j for some j provided this r of x j this will not be belongs to in the (Refer Time: 25:46). Then from here, one can calculate r of x j, so that means, if the t users is coming together then because this polynomial f polynomial is of degree t. So, if the t user is coming together then they can compute this polynomial or polynomial at some point and then they can easily get this session key. So, this can be extended for a t n thresholds secret sharing scheme also.

Thank you.