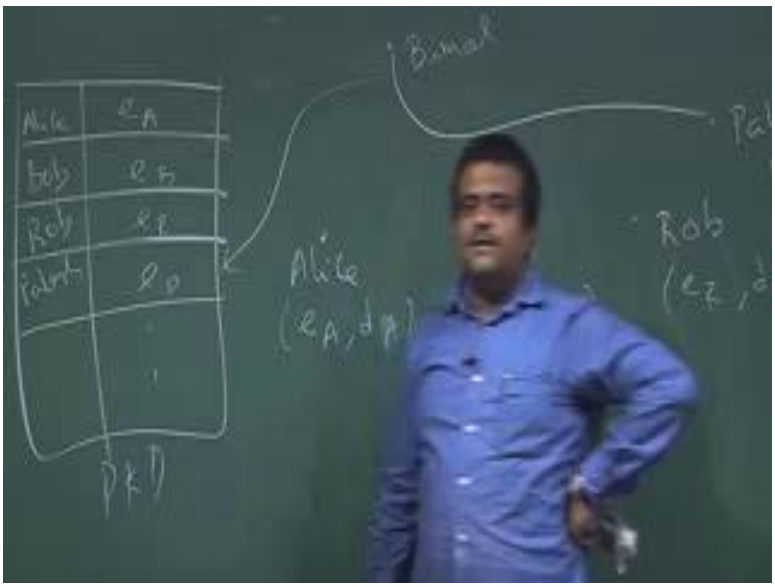
Internetwork Security
Prof. Sourav Mukhopadhyay
Department of Mathematics
Indian Institute of Technology, Kharagpur

Lecture - 54
Identity - Based Encryption (IBE)

(Refer Slide Time: 00:27)



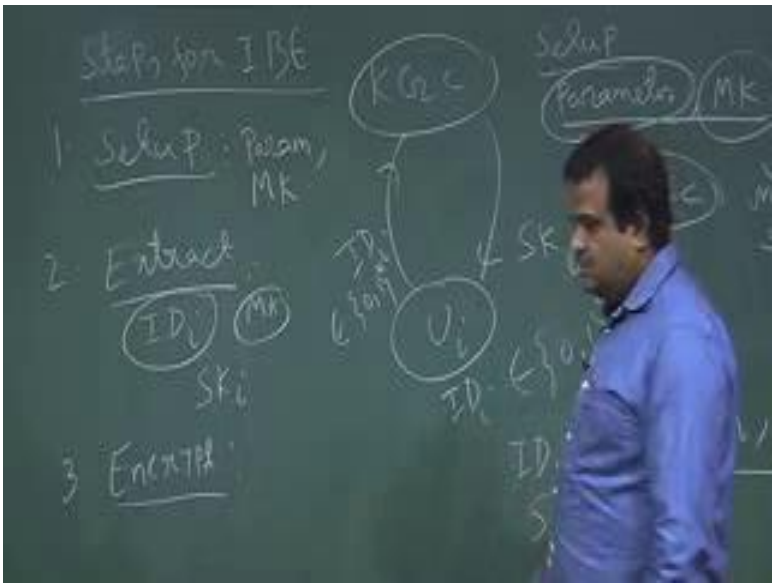
So, identity-based encryption, so this was introduced by Shamir in 1984. So, the idea is to use the ID as a public key. So, because in the public key setup what we have? We have many users say Alice, Bob, Rob, Palash. And in the public key cryptosystem, so we need to have everybody needs to have a public key, private key pair; e B, sorry e R, d R, e P d P. And then everybody's public key should be store somewhere which is a public key directory –PKD, which is storing the public key of Alice, Bob, Rob.

So, e A, so it is a long message long string; so e B, e R, e P and so on. So, in usually in public key setup, so this public key directory has to maintain; and problem there are many source like who will so anybody can. So, this should be publicly available. So, there is question of trusted party. So, who we can trust to maintain this public key directory and then again asking the public key, so these are the so or certificate or we can have a public key certificate.

So, if somebody wants to send, suppose Bimal wants to send a message to Palash. So, Bimal has to get the public key for the Palash. So, Palash has to show Bimal that this is

my certificate public key certificate. So, this is a very to get rid of this headache, so Shamir introduced this identity-based encryption. So, we use the identity as a public key. So, basically we use the identity as a public key and to get the corresponding secret key.

(Refer Slide Time: 03:34)



Key generation center, there is a key generation center. So, this is a user, so U i. So, user is having a identity. So, identity also need to convert into 0, 1 string. So, what user will send user will send this ID to this key generation center; and the key generation center will give the. The key generation center choose some this is the set up phase choose some public parameter we will discuss what are these by an example this is parameter, and it is having a master key which will be used to get the secret key corresponding to that users. I mean which will be used to get the secret key corresponding to that ID.

So, it is sending the ID which is basically 0, 1 string of any length. And it should give us the secret key of U i and then the this pair S K i. ID is the e I, and this S K i is the d I, so this is the public key and secret key pair of this. And, but when the encryption will be done, in the encryption we need to use the public parameter. This parameter set is public, but this is the master secret key of the key generation centre. This is the master secret key, which will be used for generating the secret key corresponding to the id.

So, basically it has to this step, first step is setup phase. So, steps for identity based encryption. So, first one is setup phase, we should run the setup phase or key generation phase. In the setup phase we choose the parameter - the public parameter, we say it

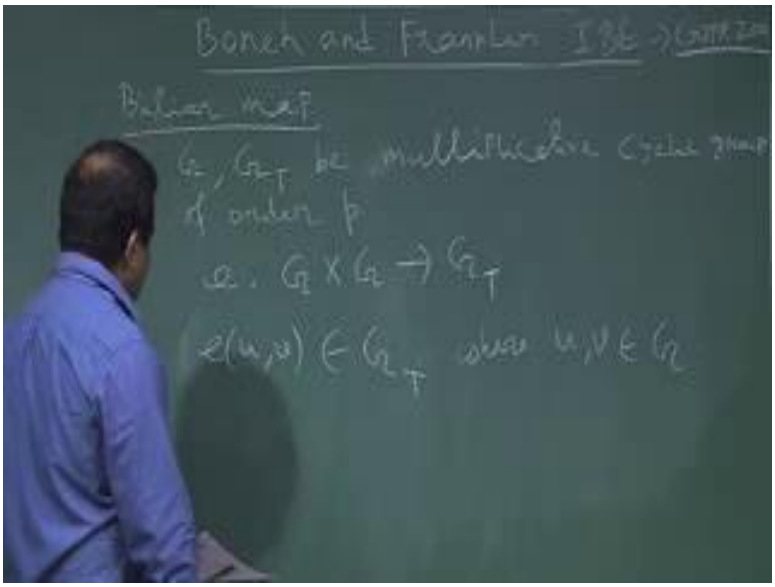
param and the master key which is secret to this key generation center. And then the key generation which is named as extract, we will extract the use the master key and the id. So, say use the master key and the id, this is the id of user one and use the master key we should able to generate the secret key of the corresponding users. And then the third step is encryption, encryption or encrypt. At the encryption, so now, we have, so this is basically.

(Refer Slide Time: 07:54)

So, now Alice wants to send a message to Bob. So, Bob is having his id. So, this ID could be ID of bob. So, ID could be say email ID a unique identification number email ID or a finger print, this biometric, the finger print could be ID of the bob we can use the finger print as the ID. So, any unique identification of that person is called id, but it has to convert into binary. So, this is the key generation center which are the setup phase choose to param, this is public and a master key which is secret. So, bob send his ID of bob and get back the bob d B. So, this is bob e B. So, bob e B, bob d B. And now this is done. So, now bob is having the public key, bob is having this. Now, Alice can send a message to Bob using this Bob public key which is getting from this and that is can be Alice can get this from the KGC key generation center also and then Alice can encrypt and send the message to Bob.

And the forth step is the decryption we will come to an example a decryption. So, this to overcome that head headache of the certificate or the public key directory. So, basically we can use the identity as a public key; identity could be email ID, biometric anything.

(Refer Slide Time: 10:23)



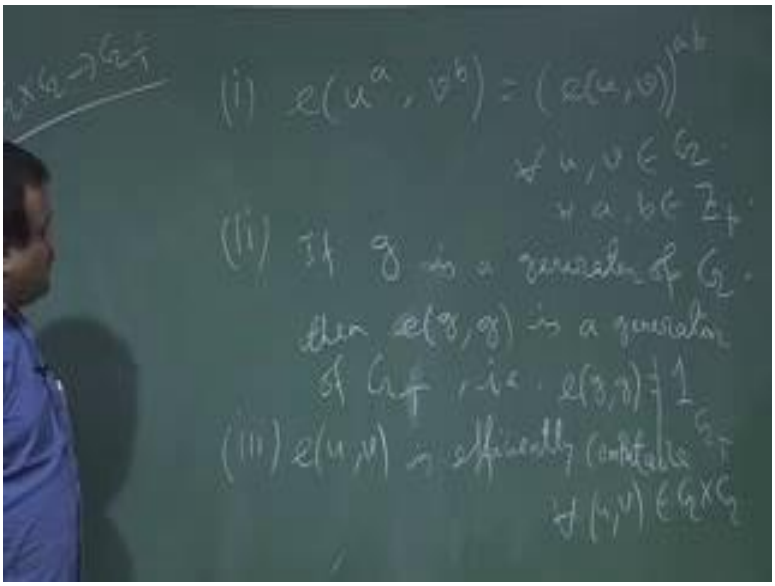
Let us talk about ID based example of a ID based encryption which is by Boneh and Franklin. And this work was published in crypto 2001, Boneh and Franklin identity based encryption, this is crypto 2001, this was established. The full paper can create from there. So, it is basically use the bilinear map. So, let us recall the bilinear map or bilinear pairing. So, suppose we have two cyclic group - G and G T 2 - two cyclic group multiplicative group, cyclic group of order p. So, we have two groups of order p G 1 and G 2. And then we defined a map e which is for sorry G and G T. And now we defined a two we defined a map from G plus G 2, G T. So, it is taking a two element from so e of u, v belongs to G T where u, v both belongs to G. So, it is basically a mapping from G cross G to G t. So, we take two elements from G and then the mapping then that will map to the element in G T.

(Refer Slide Time: 12:54)

So, these will be called a bilinear map, if it is satisfying some properties. So, what are those properties? The first property is e of u to the power a, v to the power b should be equal to e of u, v to the power a b. And this is true for all u, v belongs to G and all a b belongs to Z p. Let us understand this. So, u of a means u times u of a means u times, so this is the multiplicative group G is the multiplicative group of order p, so that means, if you take so this is basically G times a times. So, this is also will be belongs to G.

Similarly, v is belongs to G so that means, if you operate v, v times v into v into v b times. So, this is basically v to the power b this will be also belongs to G. So, if these two belongs to G then we can talk about they are e, I mean the map because map is defined for G cross G to G T sorry. So, we can talk about this mapping that. This should be equal to e of u, v to the power a b. So, this a b means this dot is basically modulo operation of modulo p over the Z p that is our underlying field. So, this is the first property. So, it must satisfy this bi linearity property. So, this is the first property.

(Refer Slide Time: 15:19)



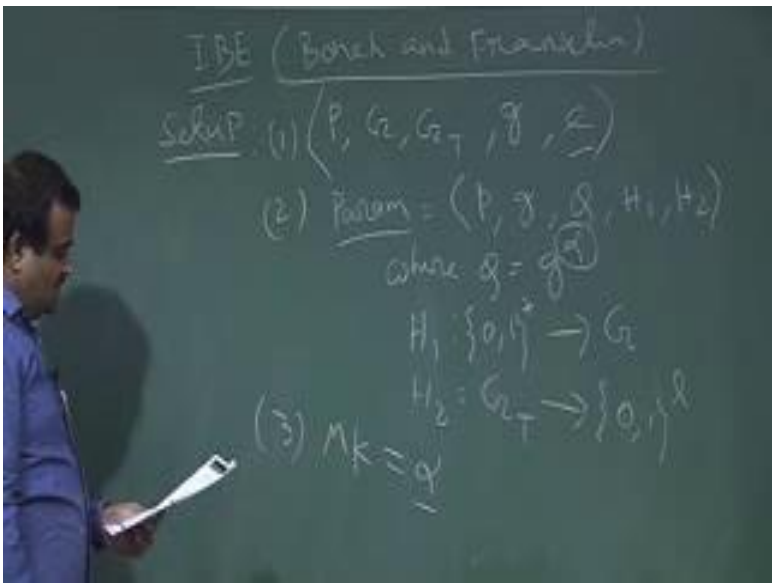
And if G is a generator, and then e g, g should be generator of G T. So, second thing is if g is a generator of G then e g, g is a generator of G T so that means e g g should not be equal to 1, 1 in G T I mean identity element in G T. If it is identity element, it cannot generate the group. So, this should not be equal to identity element of G T. So if g is the generator of this then e g g is the generator, so this we have seen.

Now, the third property is we should have some algorithm to compute this e u, v for all u, v is efficiently computable for all u, v belongs to G cross G; otherwise nobody will. We should able to compute this actually. So, if this properties are satisfying then we called this is the bilinear map, and this we have used for joux protocol if you remember for key exchange for a three party key exchange in a single round.

(Refer Slide Time: 17:30)

So, now the example of such a map is so this we can taken known, but this is not in our syllabus this example Tate pairing and Weil pairing from the elliptic curve. These two are example of bilinear map, but it involves some algebra divisibility theory to develop this Tate pairing and Weil pairing. But this course we are not going to the details of this construction, but we will use this for our construction of IBE.

(Refer Slide Time: 18:25)



So, we will use this bilinear map in IBE, Boneh and Franklin. So, this is the Boneh and Franklin. So, setup phase. So, at the setup phase, we choose a P and G, G T and g is a

generator and e bilinear map. So, this P is prime, and G and G T are two multiplicative groups cyclic group of order p, and g is a generator of G, and e is the bilinear map. So, this is we choose. And then we define the parameter public parameter as this p, g, q we defined q and two hash functions H 1 and H 2. So, what are H 1 H 2 where Q is basically G to the power of alpha, alpha should be the master key. And H 1 is the hash function which takes the any.

So, this is basically this will convert the ID to element in G, so, these two G. So, it will because ID could be anything a biometric - finger print then finger print has many char characteristic in this. So, I think forty or some possibilities are there. So, then we can convert into matrix then we can convert into this is basically an image, we can convert into matrix and then that matrix we can convert into a vector like this, so anyway. So, this is basically any arbitrarily length 0, 1 vector and then it will convert to a group element G. So, this is the hash function we use. And another hash function is basically it takes an element in G T and it will convert into l bit length. So, this is the public parameter and the master key is basically this alpha, this alpha is a master key. Now, this is the setup phase.

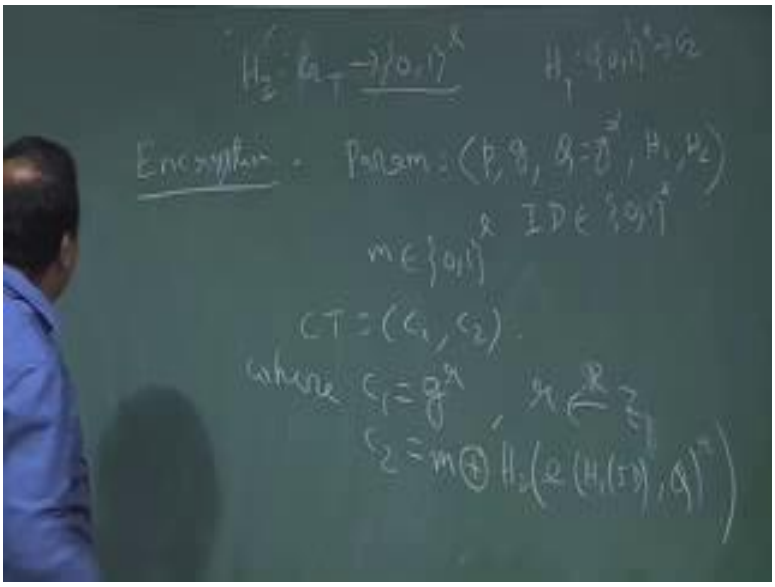
(Refer Slide Time: 21:25)

So, now, let us talk about how to get the secret key for the users. The public key, so this is the key generation center, and we have users over here U i. So, it is having the param, and the master key now it sends the id. So, id is basically this must be a zero one string e

it is a biometric we convert into a 0, 1 string. It is email id, so we convert into ASCII value then we convert into binary string. So, everything can be converted into binary string by a proper correspondence.

Now, what will be the secret key? So, secret key of this users is basically H 1 ID i to the power alpha. So, this is the secret key of the user. So, basically, so H 1, so we take the id, if you remember H 1 is a from it is take any arbitrary size length convert to the some element in G. So, this will be the G element in G, now we can take to the power alpha. So, this is basically the secret key of this id. So, this is the key generation. So, we got the id of the users.

(Refer Slide Time: 23:20)

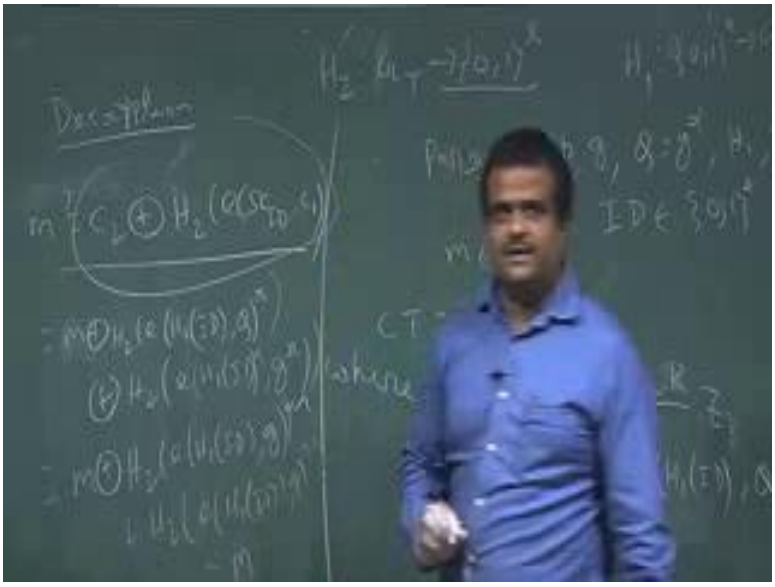


Now, what about encryption? So, through encrypt, we need the public parameter. So, just recall we need to have this public parameter; it is basically p comma g comma q which is basically g to the power alpha H 1 H 2. And we have the ID, which is the public key of the users and the secret key of the users is we got from this key generation center.

So, and the message is basically a length of l bit. So, it is generate a ciphertext C T, which is have two parts c 1 and c 2 it is similar to the elgamal encryption. C 1 and C 2 where C 1 is basically g to the power r, r is chosen randomly from Z p. So, this means randomly for Z p. So, this is C 1 and C 2 other part of the ciphertext is basically I am asking m XOR with H 2 of e of H 1 of ID, if we take the H 1 of I D it will be element in G and then we have q, q is basically G to the power r.

So, these to the power r and then after this we take the H 2 on this. So, this will be an element in G T because this is basically H 1 of this is an element in G and this is an element in g. So, this will be an element in G t. So, this will be an element in G T and then H 2 will convert into again H 2 is a mapping from if you recall H 2 is basically a hash function G T to 0, 1 to the power l because all matches is l bit. So, we can do the XOR with this. So, this is the encryption which Alice is doing for Bob. So, Alice is sending this message to Bob.

(Refer Slide Time: 26:14)



Now, how bob will decrypt it. So, this is encryption. So, decryption is basically, so how Bob will decrypt it. So, Bob will just give this thing m is basically, so bob is receiving C 1, C 2. So, Bob will just do m is basically C 2 XOR with H 2 of e of S K I D comma C 1 e of s. So, this is the Bob's secret key. So, Bob's secret key and C 1 it is getting from the ciphertext. So, it will compute this e of S K I D and C 1 and apply H 2. So, H 2 will be again a l bit and this should give us m.

So, what is the correctness? So, if you just check this, this quantity, so this should be m. So, if you just check this quantity this is basically C 2 basically what, C 2 is basically m XOR with this m x or with H 2 of e of H 1 of ID Q to the power r. This XOR with we are doing H 2 of e of H 1 of this is basically ID to the power alpha and G to the power r. So, this is basically m XOR with, so this term will be same, so H 2 of e of H 1 I D G to the power alpha r and H 2 of same thing, e H 1 I D comma G to the power alpha r. So, these

two will give us m. So, this is the correctness of this. So, we will get the message. So, this is the identity-based encryption where we will use the ID as a public key to avoid this certificate or to maintain this public key directory. So, ID could be anything finger print or any email ID or any unique identification of the users.

Thank you.