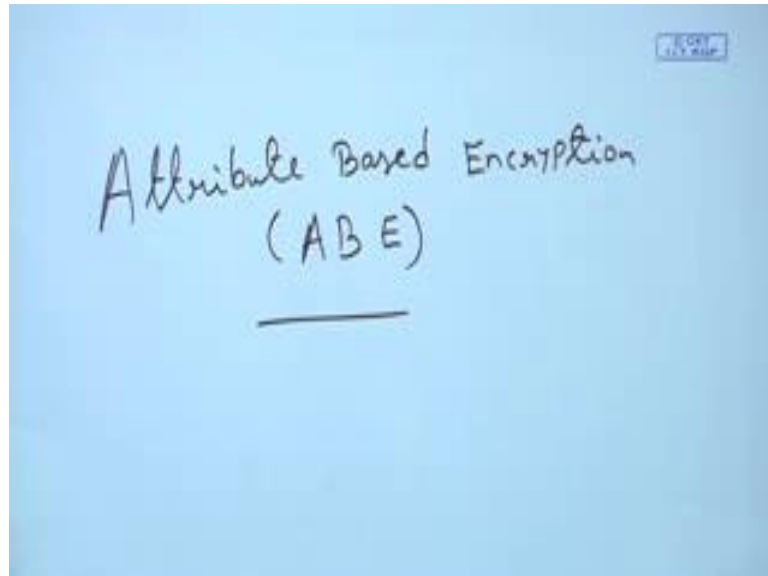


Internetwork Security
Prof. Sourav Mukhopadhyay
Department of Mathematics
Indian Institute of Technology, Kharagpur

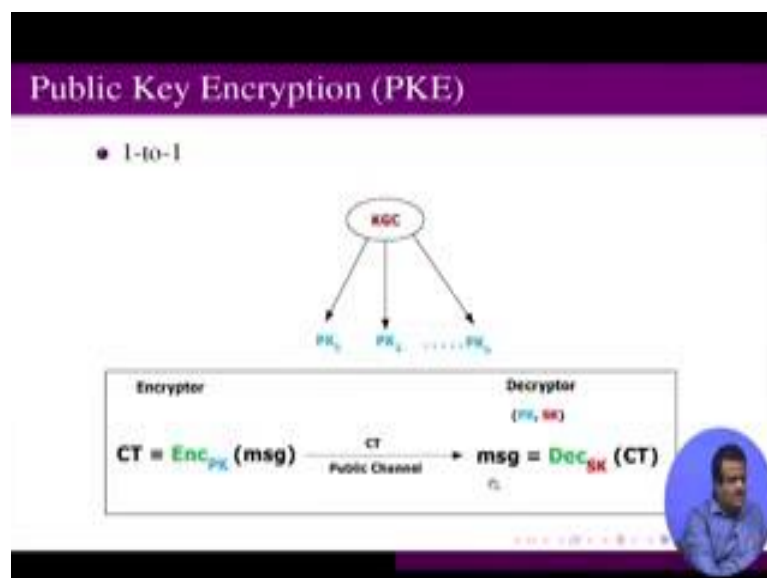
Lecture - 55
Attribute Based Encryption

(Refer Slide Time: 00:23)



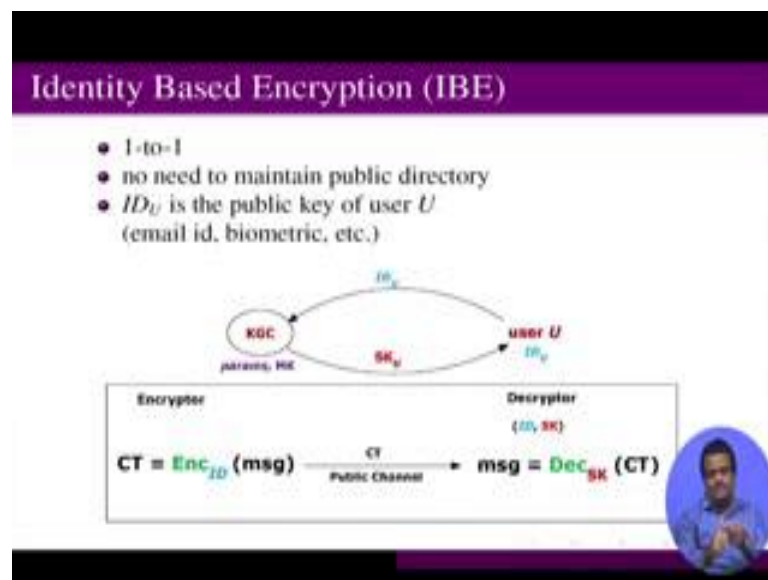
So, we talk about Attribute Based Encryption. There we will see how we can use the attributes to encrypt.

(Refer Slide Time: 00:32)



So, this is the basically public key encryption setup public key PKE setup. So, in public key what we have seen it is a basically one to one. So, we have a public key generation center, which give us public keys or we can have I mean every user is having its own public key private key pair. So, while encryption is done using the public key of the users, on the message, and send it to the public channel this ciphertext and this message will be recovered by the decryptor and this decryptor is having the public key and the corresponding secret key. And then using the decryption algorithm on the ciphertext using the secret key or the private corresponding private key the users get the message. So, this is one to one correspondence.

(Refer Slide Time: 01:32)



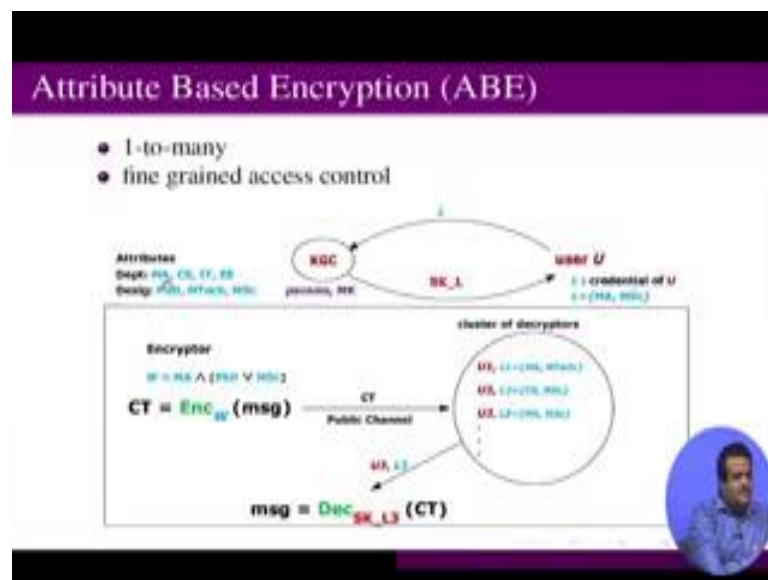
Then we discuss the identity based encryption scheme where this is also one to one correspondence, but here we do not need to maintain any public key directory, we can just use the ID of the users as a public key. And to get this id could be email id biometric, I mean our finger print, finger print could be the id I mean like this we the thumb impression, or our retina it could be the id. So, any biometric or any email id, so this should be the unique identification I mean our PAN number, so our email id. So, any unique identification can be used as id of the users.

So, in this identity based encryption scenario, we use the users is having his own id. So, user will send the id to the key generation center, and the key generation center is having this is at setup face having a parameter - public parameter and the master key, and this

master key will be used to generate the say secret key of the users. And this key generation center will send the secret key of the users. So, this id is public key and the SK is the secret key. So, this basic difference is basically identity, we are using as a public key.

And the encryption is by similar way suppose this is Alice this is Bob, Alice wants to send a message to Bob. So, Alice will need to get the Bob's public key, but now here public key is basically id, so Alice not Bob id. So, Alice will use Bob id along with the public parameter need to use and generate the ciphertext - CT, and send it over the public channel. Now, Bob is having Bob secret key SK. So, Bob will decrypt this by applying the description algorithm and then get this message which is send by the Alice.

(Refer Slide Time: 03:51)



Now, this was earlier every scheme was the one to one scheme. So, now, this is basically for one to one scheme, we have a difficulty to suppose we want to send a message, so that all that legitimate users will able to decrypt it. So, for that, so one to one will create some problem because the bandwidth will be more, because we have to send to everybody, so in that way, so these attribute base encryption is basically one to many, so basically it is a fine grained access structure. So, here the scenario is every user has a credential of the users. So, suppose we are talking about student database, so user is a student. So, that student is MA - mathematics, MA means mathematics department

student or maths student, and M.Sc. - the student is enrolled as a M.Sc. student. So, this is the one is the credential of this of this user.

Now, this user will send user credential to the key generation center and the key generation center at the setup phase it is having the public parameter and the master key and using it will send the secret key for this credential, so SK L. So, it will send the secret key with that credential of the users. Now, the attributes are basically departments it is the MA, computer science, IT, EE these are the attributes. Then the codes which is enrolled like whether it is PhD, M. Tech, M.Sc., so these are the basically designation of the student, so whether M.Sc. enroll.

So, now, we want that encryption should be done if this attributes is satisfied. These attribute means this student should be MA, and this student is either PhD student or M.Sc. student. So, we want to broadcast a message so that only those students which is having satisfying the attributes, attributes is basically the student is mathematic department student and student has he is a PhD student or student is a M.Sc. student. So, this is the attribute. So, if these attribute is satisfy then the student that student should able to decrypt it. So, this has many applications in the say cloud computing system. So, we put our data in the cloud in encrypted way. So, now, we want that we some group of student should able to see the data.

So, suppose we release the marks of the students. So, now, we release the marks of the M.Sc mathematic M.Sc students the marks sheet, I mean like the role list on this. So, we will use this attribute based encryption. So, we broadcast this ciphertext, we encrypt it and we broadcast it, but we only allow those students who are mathematic student and M.Sc, they should able to decrypted to see their marks. So, this is the attributes we are giving. So, if these attributes satisfied by the users then he or she all they should be able to decrypt it, so that is the idea.


So, this W is the basically MA and so we encrypt the message using this set of attributes W and this generate the ciphertext. And this we broadcast over the public channel. Now, this is the cluster of decryptor, this is the group of users - u_1, u_2, u_n . So, this is say u_3 this with they have the credential like MA, M.Sc, so these group should able to decrypt the message using their secret key based on that credential L. So, this secret key will be

received by the key generation center based on their attribute attributes I mean their credential.

(Refer Slide Time: 08:32)

Applications

- Cloud Storage Applications
- Disruption-Tolerant Networks
- Wireless Sensor Networks
- Mobile Ad Hoc Networks
- Internet Services



So, these has good application as I said could storage applications, and tolerant networks, wireless sensor network, mobile ad hoc network and internet services, we may talk few more details in the latter lectures.

(Refer Slide Time: 08:46)

Broadcast Encryption (BE)

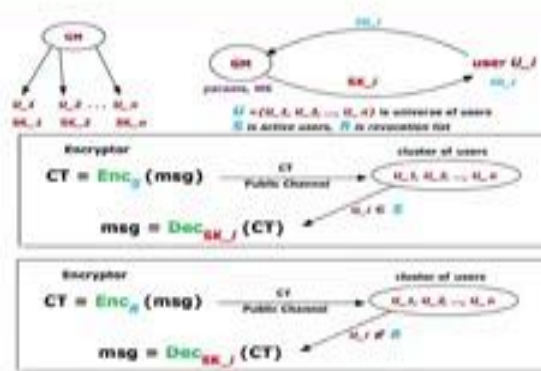



Diagram illustrating Broadcast Encryption (BE):

- Key Generation Center (KGC)** distributes keys SK_1, SK_2, \dots, SK_n to users U_1, U_2, \dots, U_n .
- Cluster of users** U_1, U_2, \dots, U_n .
- Encryption:** $CT = \text{Enc}_K(\text{msg})$ (Public Channel).
- Decryption:** $\text{msg} = \text{Dec}_{SK_j}(CT)$.
- User U_i :** $U_i \in \mathcal{U}$ (Active users), $U_i \notin \mathcal{R}$ (Revocation list).



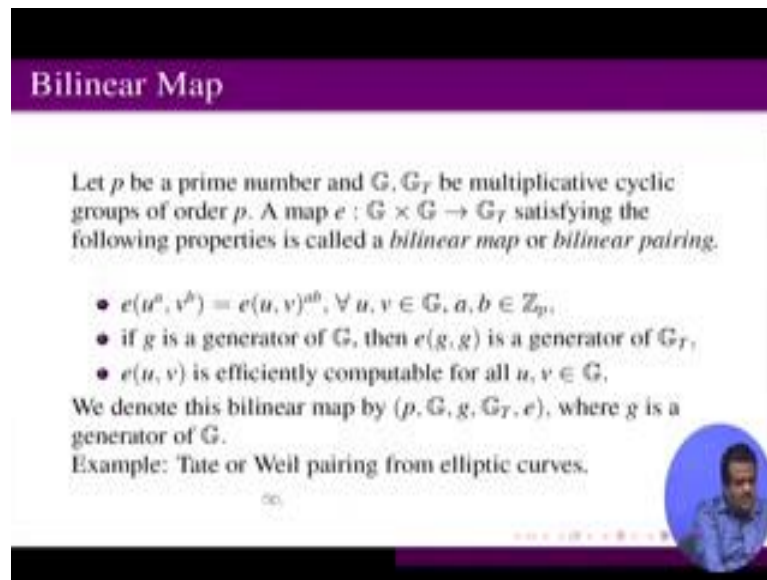
So, now this is another one to many, which is broadcast encryption. So, in broadcast encryption, what we have, we have a group manager or some say for cable operator, we

have a group dealer I mean we have a dealer or the group manager and there are some users and users are having some secret keys some secret SK 1, SK 2, SK L like this. So, now, a user how they regard this secret they user U I will send the identity of it is, to the group manager and group manager send the secret SK I to the user I. So, then this is the set of users universe of the user among this set S is the active user. So, few users can revoke. So, R is the setup revoke user few user could be revoked.

So, suppose for example, if it is some TV service provider some cable operator, so there are few users, who are subscribers for this channel and there are few users who stop paying, so those are basically revoked user. So, those are basically set of revoked user, but still there are some users which are active user; that means, they are not revoked user. So, they should be the legitimate user. So, they should be able to decrypt the encrypted channel information or encrypted movie, so that is the idea.

So, in here S is the active user, and R is the revoke revoked user list. And so the encryption will be done in this way either two possibilities are there, two ways we can do this broadcast encryption. The first one is we can use the set of active users while encrypting and generate the ciphertext and broadcast it and this is the group of users. So, among this if U I's belongs to the set of active user then only U I's able to decrypt it. So, this is one way or we can use the set of revoked user list R, and we generate the ciphertext using the set of revoked user list and this broadcast the ciphertext over the public channel and only the users which are not revoked user should be able to decrypt using its own secret key. So this is the broadcast encryption.

(Refer Slide Time: 11:43)



Bilinear Map

Let p be a prime number and G, G_T be multiplicative cyclic groups of order p . A map $e : G \times G \rightarrow G_T$ satisfying the following properties is called a *bilinear map* or *bilinear pairing*.

- $e(u^a, v^b) = e(u, v)^{ab}, \forall u, v \in G, a, b \in \mathbb{Z}_p,$
- if g is a generator of G , then $e(g, g)$ is a generator of G_T ,
- $e(u, v)$ is efficiently computable for all $u, v \in G$,

We denote this bilinear map by (p, G, g, G_T, e) , where g is a generator of G .

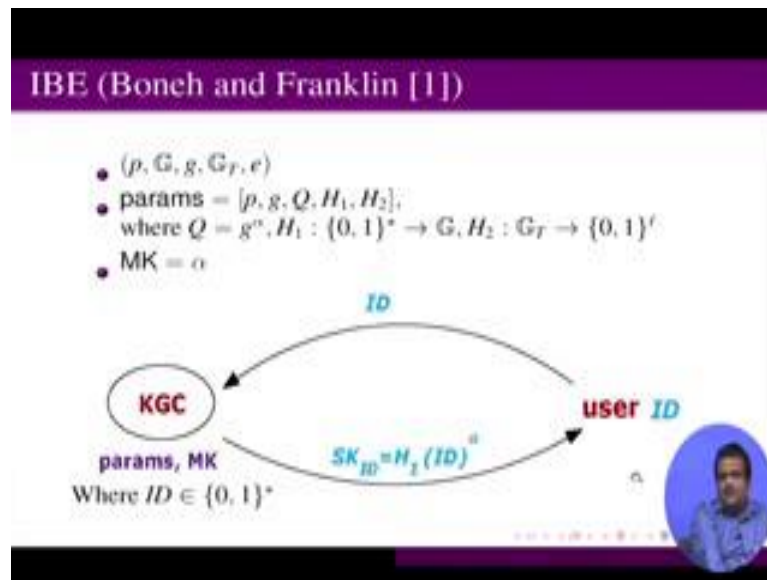
Example: Tate or Weil pairing from elliptic curves.

Navigation icons: back, forward, search, etc.

So, we will see some scheme of this broadcast encryption. For that we need to use this bilinear map. So, just to recap, so let G and G_T be multiplicative cyclic group of order p and p is a prime. So, e is a map from G cross G to G_T satisfying the following property first properties $e(u^a, v^b)$ should be equal to $e(u, v)^{ab}$, because u to the power a means u times a . So, a belongs to \mathbb{Z}_p . So, e to the power a is a belongs to G and similarly v to the power b will also belongs to G , so $e(u, v)$ to the power ab . So, this we can operate e on this because e is the mapping from G cross G to G_T . So, we operate this, so this should be called this is the validating property.

And if g is the generate of G , small g is the generator of capital G then $e(g, g)$ should be is a generator of G_T so that means, $e(g, g)$ should not be equal to the identity element to the G_T . And $e(u, v)$ should be efficiently computable so that means, there should adjustable polynomial time algorithm to compute $e(u, v)$, you should just practical example of compute of this $e(u, v)$. So, for example, Tate pairing or Weil pairing from elliptic curves are basic two example of this bilinear map, but this involves the algebra like a divisibility theory of all this thing. So, for this course this is not in our syllabus, but we will only use the concept of the bilinear map in a theoretical way. So, we are not going to the details of construction of this $e(u, v)$, but this is two example if you have interest you can look into the details of this, but it make some math background.

(Refer Slide Time: 13:54)



So, let us come to the identical encryption scheme from Boneh and Franklin, which was published in crypto 2001. So, this we have already discussed. So, just to recap, so here this is the this is G , g , G_T and small g is the generator of G , and p is a prime number, e is a bilinear map. And this public parameter is p, g, Q - Q is basically g to the power α . So, α is the master key which will use for generating the secret key of the users. And H_1 is the mapping, H_1 is the hash functions which take the any arbitrary input and generate element in G . And H_2 is a mapping a hash function from which take element in G_T and give a 0 1 bit of length l . So, this is the identity base encryption to users sales id to the PKC public key generation center of key generation center. And using this public parameter and the master key, so this PKG will send this H_1 id to the power α as the secret key of the user whose id is ID .

(Refer Slide Time: 15:21)

IBE (Boneh and Franklin [1])

Encrypt(params = $[p, g, Q = g^\alpha, H_1, H_2], ID \in \{0, 1\}^*, \text{msg} \in \{0, 1\}^l$)

- $CT = [C_1, C_2]$
 - where $C_1 = g^r, C_2 = \text{msg} \oplus H_2(e(H_1(ID), Q)^r), r \xleftarrow{R} \mathbb{Z}_p$.

Decrypt(params, $SK_{ID} = H_1(ID)^\alpha, CT$)

- $\text{msg} = C_2 \oplus H_2(e(SK_{ID}, C_1))$

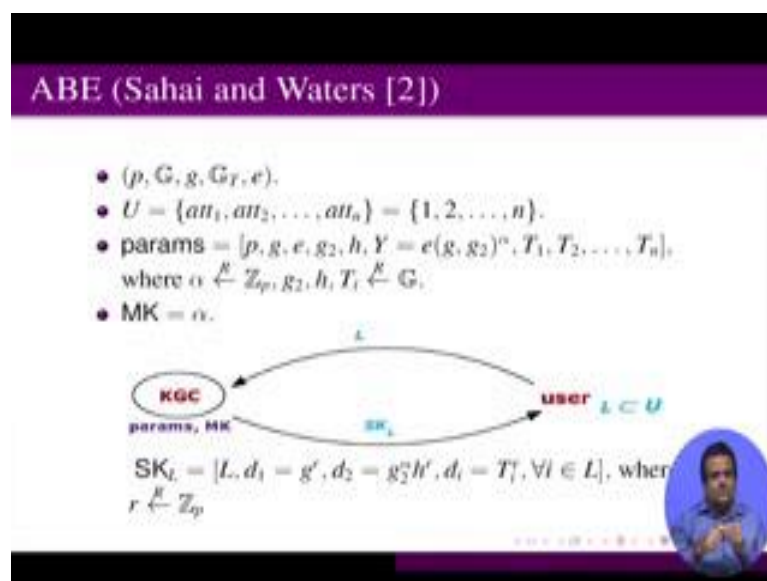
Correctness:

$$\begin{aligned}
 & C_2 \oplus H_2(e(SK_{ID}, C_1)) \\
 &= \text{msg} \oplus H_2(e(H_1(ID), Q)^r) \oplus H_2(e(H_1(ID)^\alpha, g^r)) \\
 &= \text{msg} \oplus H_2(e(H_1(ID), g^\alpha)^r) \oplus H_2(e(H_1(ID)^\alpha, g^r)) \\
 &= \text{msg} \oplus H_2(e(H_1(ID), g)^{\alpha r}) \oplus H_2(e(H_1(ID), g)^{\alpha r}) \\
 &= \text{msg}
 \end{aligned}$$

So, now the encryption is this way. So, this is the ciphertext C_1, C_2 . So, we generate a random number R from the \mathbb{Z}_p . So, we compute g to the power r and C_2 is basically this is the message. So, C_2 is basically XOR with this H_2 applied on this $e(H_1(ID), Q)$ to the power r , and this is basically C_1 and C_2 . So, this C_1 and C_2 will be sent it to the receiver.

Now, receiver will receive, the receiver is having also public parameter is public, and receiver is having this secret key which is basically $H_1(ID)$ to the power α and getting the ciphertext CT over the public channel. Then receiver can be decrypt this by just applying C_2 XOR with $H_2(e(SK_{ID}, C_1))$, because this basically will be give us this. C_2 is basically message XOR with this, and now if you just calculate this H_2 of this H_2 of e of $H_1(ID)$ comma Q to the power r XOR with H_2 of e of $H_1(ID)$ to the power α to g to the power α . Now, we can use the bilinearity property of this. So, it will, the basically αr , and similarly this will be also αr . So, these two will be cancel out and will be getting the message, this thing. So, this is the identify encryption we have seen.

(Refer Slide Time: 17:01)



Now we will talk about attribute base encryption where this is Sahai and Waters. So, this is basically called fuzzy identity based encryption, why fuzzy identity based encryption? Because suppose we are using the identity as the biometric, so our finger prints, so our finger print means it has some characteristic over here. So, based on that I think 40 characteristic are there to, based on that characteristic it uniquely determines of finger print. So, suppose we have some card or something, so may be all characteristic are not matching. So, suppose few or matching. So, even though we should able to decrypt it so that means there is the threshold. So, that is why it is called fuzzy identity base encryption.

So, we have a some threshold orbit, so that threshold if d many characteristics matching in the finger print then we should able to decrypt it, so that way. So, this is basically a case of attribute base encryption. So, let us talk about Sahai and Water attribute encryption. So, this is basically having this set of phase, we choose p, G same as same way. And these are the attributes, so 1, 2 up to n , these are basically those forty characteristics of the finger print like which uniquely determined the finger print we can say. And these are the public parameter p, g, e, g_2 then h is the hash function we use and Y , Y is basically $e(g, g_2)^\alpha$ and this T_1, T_2, T_n where T_1 are basically randomly chosen from the G . So, they are the element from G , which is randomly chosen. And α is the randomly chosen from \mathbb{Z}_p which will be the master key, so this is the master key.

So, now what we will do we will send a credential. So, user will send a credential L to the center group KGC - key generation center; and key generation center will send a SKL to the users. The SKL is basically L comma d_1 ; d_1 is basically g^2 to the power r ; d_2 is basically g^2 to the power αh_1 to the power r ; d_i is basically T_i to the power r . This T_i 's are basically randomly chosen and this where r is also randomly chosen from \mathbb{Z}_p . So, this is basically secret key send to the user. So, if we use this credential in the encrypted form, so if they are coming together it should be able to decrypt it, so that is the idea of attribute based encryption.

(Refer Slide Time: 20:12)

ABE (Sahai and Waters [2])


Encrypt(params $[p, g, e, g_2, h, Y = e(g, g_2)^\alpha, T_1, T_2, \dots, T_n]$,
 $W = i_1 \wedge i_2 \wedge \dots \wedge i_k, \text{msg} \in \mathbb{G}_T$)

- $\text{CT} = [W, C_1, C_2, C_3]$,
 where $C_1 \equiv \text{msg} \cdot Y^s$, $C_2 = g^s$, $C_3 = (h \prod_{j=1}^k T_{i_j})^s$, $s \xleftarrow{R} \mathbb{Z}_p$

Decrypt(params, $\text{SK}_L = [L, d_1, d_2, d_i, \forall i \in L]$, $\text{CT} = [W, C_1, C_2, C_3]$)

- If $\{i_1, i_2, \dots, i_k\} \not\subset L$, decryption fails
- If $\{i_1, i_2, \dots, i_k\} \subset L$, then $d = d_2 \prod_{j=1}^k d_{i_j}$ and

$$\text{msg} = \frac{C_1 \cdot e(d_1, C_3)}{e(d, C_2)}$$



So, this is the encryption part. So, in the encryption part, we need use the public parameter. So, these are the public parameter. And this is basically the message we are going to encrypt. So, message belongs to \mathbb{G}_T . And this is the ciphertext. So, ciphertext has few components - W, C_1, C_2, C_3 . So, C_1 is basically we just give the message and dot Y to the power s ; C_2 is basically g^2 to the power s ; C_3 is basically this h of this to the power s ; and this s is randomly chosen from this \mathbb{Z}_p .

And this decryption is basically for decryption we also need the public parameter and the SKL, SKL is the secret key received from this key generation center upon the sending this credential of the users. And with the ciphertext CT by just using if this i_1, i_2, i_1 belongs to L this credential or it not a subset of L then decryption must fail. But if it is subset of L , so that means, if our finger among the finger print if d many characteristics

satisfy then it should be able to decrypt it, so that means, you are allowing that is why it is called fuzzy, fuzzy identity base encryption. So, we have we are given a threshold. So, threshold is t . So, t is the threshold. So, if it is satisfied, then we should be able to decrypt it. So, this decryption is just by simply C_2 into $e(d, C_3)$ divided by $e(d, C_2)$.

(Refer Slide Time: 22:14)


ABE (Sahai and Waters [2])

Correctness

- $SK_L = [L, d_1 = g^r, d_2 = g_2^s h^r, d_i = T_i^r, \forall i \in L]$
- $CT = [W, C_1 = \text{msg} \cdot Y^r, C_2 = g^r, C_3 = (h \prod_{j=1}^k T_{ij})^r]$,
where $Y = e(g, g_2)^s$ and $d = d_2 \prod_{j=1}^k d_{ij}$

$$\frac{C_1 \cdot e(d_1, C_3)}{e(d, C_2)} = \frac{\text{msg} \cdot e(g, g_2)^{rs} \cdot e(g^r, (h \prod_{j=1}^k T_{ij})^r)}{e(g_2^s h^r \prod_{j=1}^k T_{ij}^r, g^r)}$$

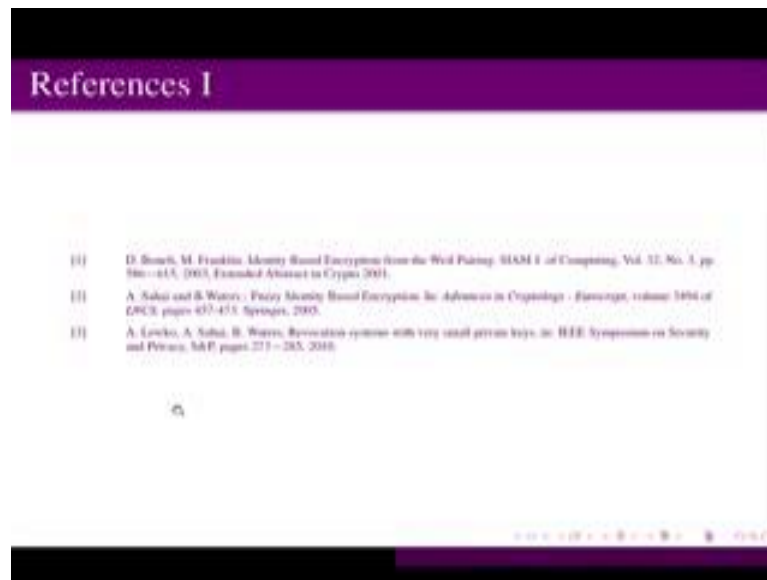
$$= \frac{\text{msg} \cdot e(g, g_2)^{rs} \cdot e(g, h \prod_{j=1}^k T_{ij})^r}{e(g_2^s, g^r) \cdot e(h \prod_{j=1}^k T_{ij}, g)^r}$$

$$= \text{msg}$$


So, this is the correctness of it. So, we have this secret key and we have the ciphertext. And then we generate this Y we know this. So, if we just calculate this, it will be giving us $e(g, g_2)$ to the power rs because of the property of bilinearity and $e(g, g)$ to the power rh of this will give us basically this is again because of the bilinearity property then these two will cancel out. So, it will give us the messages.

So, this is the Sahai and Waters scheme, but this is basically attribute base encryption, but it is basically used for fuzzy identity base encryption where we are allowing some threshold or in our identity I mean like we said fingerprint identity. So, if the fingerprint is not completely matching, so we are allowing some characteristic match among the forty characteristics, suppose thirty characteristics are matching of the fingerprint then we should be able to decrypt it, so that is the idea.

(Refer Slide Time: 23:30)



And these paper got, we will come to yeah this paper got accepted in Eurocrypt. So, this is the paper Sahai and Waters. So, this is the paper fuzzy identity base encryption paper; this paper got accepted in Eurocrypt 2005. So, there is another scheme which is broadcast encryption scheme with revocation, but this is we are not going to include in our syllabus. So, this is the paper and this broadcast encryption scheme we are not including in our syllabus.

Thank you.