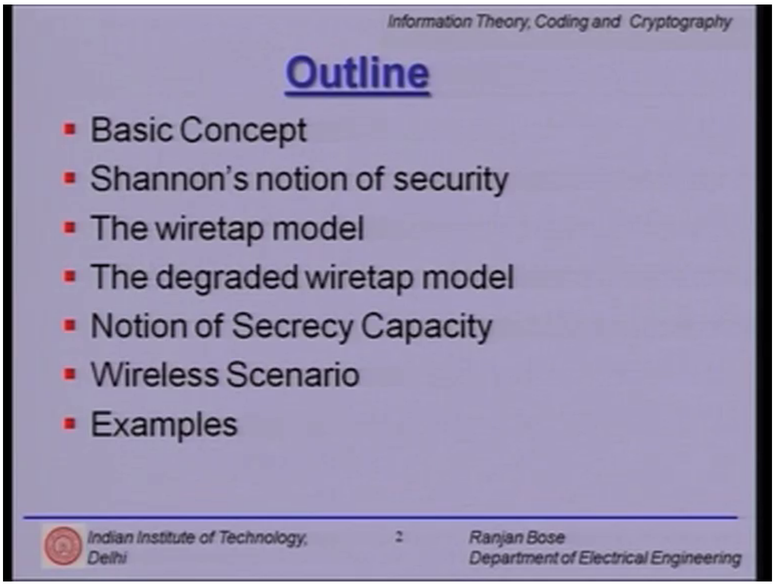
Information Theory, Coding and Cryptography
Dr. Ranjan Bose
Department of Electrical Engineering
Indian Institute of Technology, Delhi

Module – 38
Introduction to Physical Layer Security
Lecture – 38

(Refer Slide Time: 00:30)



Information Theory, Coding and Cryptography

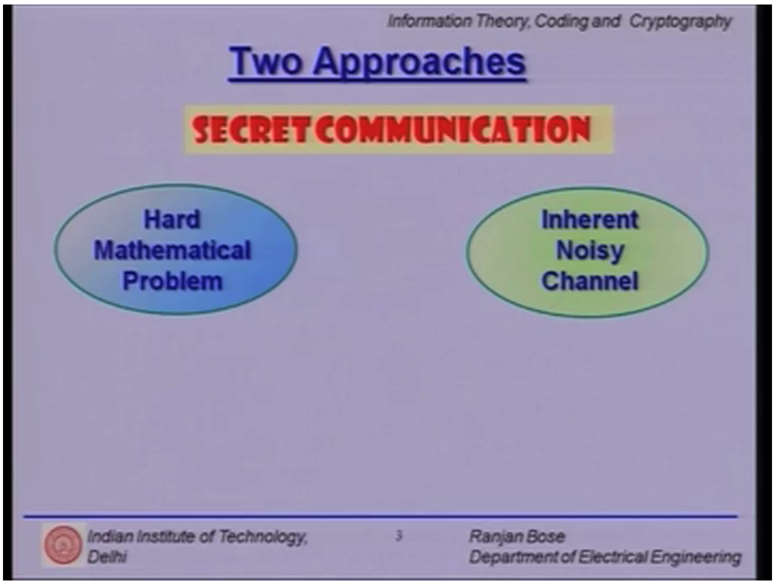
Outline

- Basic Concept
- Shannon's notion of security
- The wiretap model
- The degraded wiretap model
- Notion of Secrecy Capacity
- Wireless Scenario
- Examples

Indian Institute of Technology, Delhi 2 Ranjan Bose Department of Electrical Engineering

Hello and welcome to a lecture on Physical Layer Security. Here is a brief outline for today's talk. We will start with Shannon's notion of security. We will follow it up with the wiretap model; we will then talk about the degraded wiretap model. We will introduce the notion of secrecy capacity. Then we will talk about a practical wireless scenario. Of course we will sprinkle in some examples along the way; of course, let us first start with a basic concept.

(Refer Slide Time: 01:03)



Information Theory, Coding and Cryptography

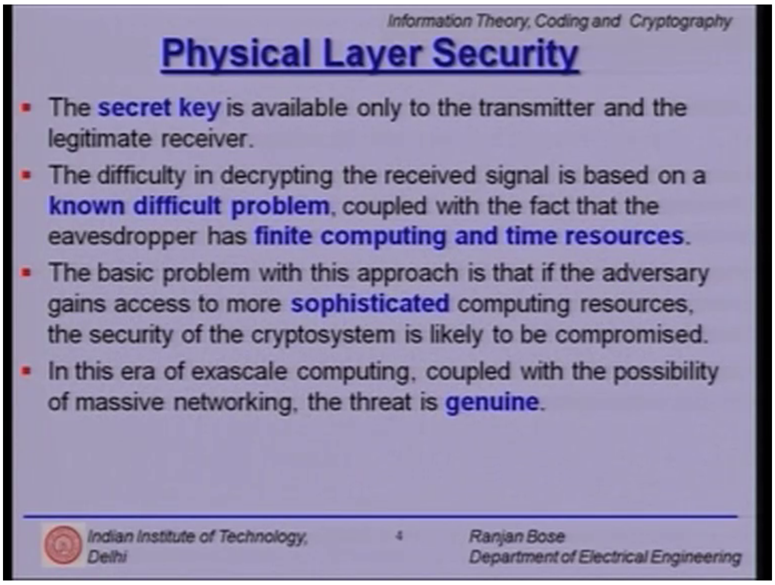
Two Approaches

SECRET COMMUNICATION

Indian Institute of Technology, Delhi 3 Ranjan Bose Department of Electrical Engineering

So, as we know secret communication can be approached from two directions. The first is to look at a hard mathematical Problem and introduce it in the communication system. So, the eavesdropper or the adversary has to solve a difficult mathematical problem in finite duration of time. The other approach is to use the inherent and noisy nature of the channel and provide security. Today's talk focuses on this approach which utilizes the inherent noisiness of the channel and uses information theoretic measures.

(Refer Slide Time: 01:50)



Information Theory, Coding and Cryptography

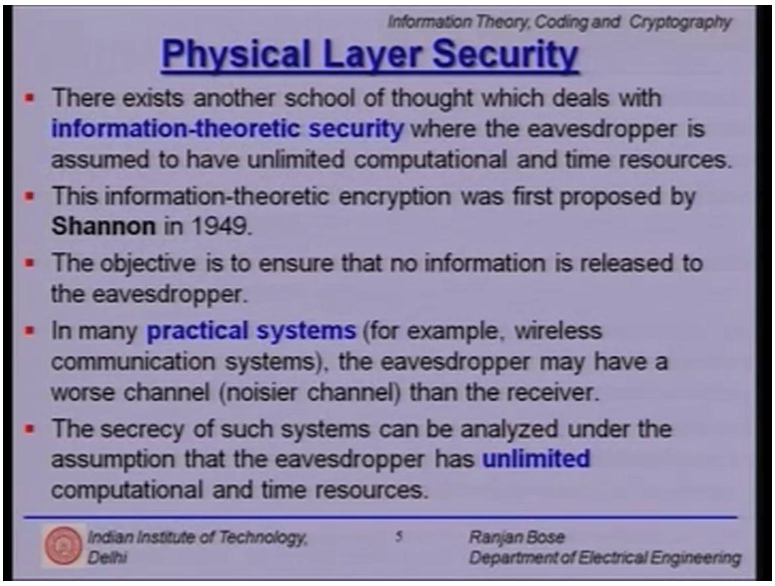
Physical Layer Security

- The **secret key** is available only to the transmitter and the legitimate receiver.
- The difficulty in decrypting the received signal is based on a **known difficult problem**, coupled with the fact that the eavesdropper has **finite computing and time resources**.
- The basic problem with this approach is that if the adversary gains access to more **sophisticated** computing resources, the security of the cryptosystem is likely to be compromised.
- In this era of exascale computing, coupled with the possibility of massive networking, the threat is **genuine**.

Indian Institute of Technology, Delhi 4 Ranjan Bose Department of Electrical Engineering

So, what is physical layer security? So, far we have assumed that there exists a secret key which is shared between the transmitter and the legitimate receiver. Now, this key is the place where security is achieved, it is it known difficult problem to solve. And we assume that there is finite computing and time resources available at the hacker. Now, the problem is that today computer systems are becoming more and more sophisticated. And in the day and age of network computing systems, the threat is genuine.

(Refer Slide Time: 02:38)



Information Theory, Coding and Cryptography

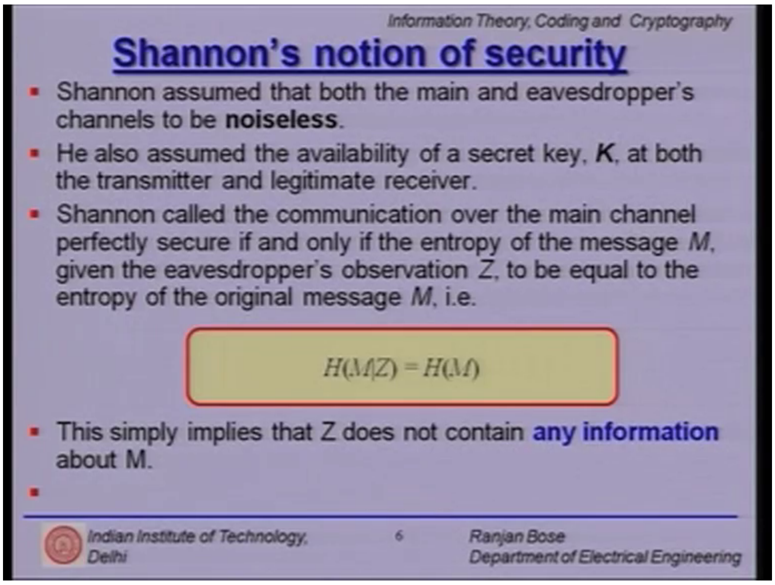
Physical Layer Security

- There exists another school of thought which deals with **information-theoretic security** where the eavesdropper is assumed to have unlimited computational and time resources.
- This information-theoretic encryption was first proposed by **Shannon** in 1949.
- The objective is to ensure that no information is released to the eavesdropper.
- In many **practical systems** (for example, wireless communication systems), the eavesdropper may have a worse channel (noisier channel) than the receiver.
- The secrecy of such systems can be analyzed under the assumption that the eavesdropper has **unlimited** computational and time resources.

Indian Institute of Technology, Delhi 5 Ranjan Bose Department of Electrical Engineering

So, the other school of thought which relies on information theoretic security does not make any assumption about the resources both computational and time available with the adversary. This information theoretic encryption was first proposed by Shannon and the idea is not to let information is released to the eavesdropper. In many practical systems, for example, in wireless communication systems, the eavesdropper may have a worse that is a noisier channel than the receiver. And we might use this advantage to communicate with a legitimate receiver secretly.

(Refer Slide Time: 03:25)



Information Theory, Coding and Cryptography

Shannon's notion of security

- Shannon assumed that both the main and eavesdropper's channels to be **noiseless**.
- He also assumed the availability of a secret key, ***K***, at both the transmitter and legitimate receiver.
- Shannon called the communication over the main channel perfectly secure if and only if the entropy of the message *M*, given the eavesdropper's observation *Z*, to be equal to the entropy of the original message *M*, i.e.

$$\boxed{H(M|Z) = H(M)}$$

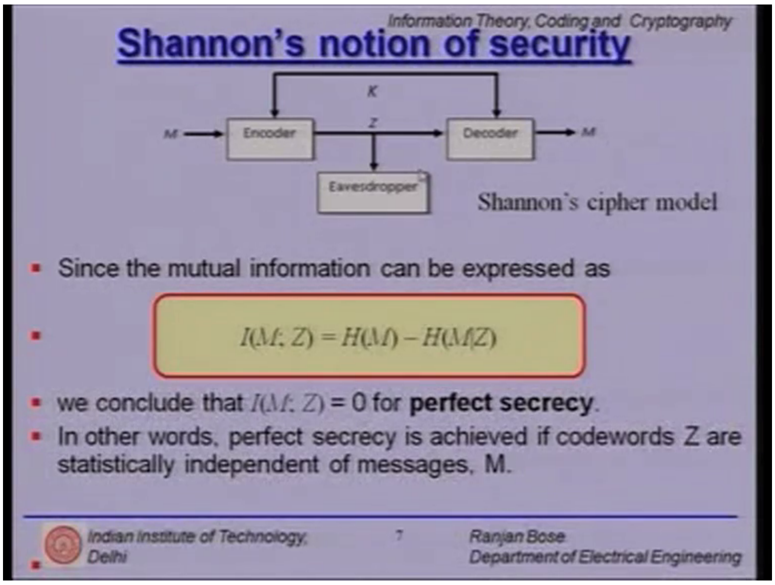
- This simply implies that Z does not contain **any information** about M.
-

Indian Institute of Technology, Delhi 6 Ranjan Bose Department of Electrical Engineering

So, let us start with Shannon's notion of security. So, the first assumptions Shannon made is that both the main and eavesdroppers channels are noiseless. So, the channels are ideal and no data is lost, because of the noise in the channel. He also assumed the availability of a common secret key between the transmitter and the legitimate receiver, but not at the eavesdropper.

So, Shannon defined his notion of perfect security if and only if the entropy of the message M given that the eavesdroppers observations Z to be equal to the entropy of the original message M that is H M given Z is the same as H M this simply means Z does not contain any information about M.

(Refer Slide Time: 04:21)



Information Theory, Coding and Cryptography

Shannon's notion of security

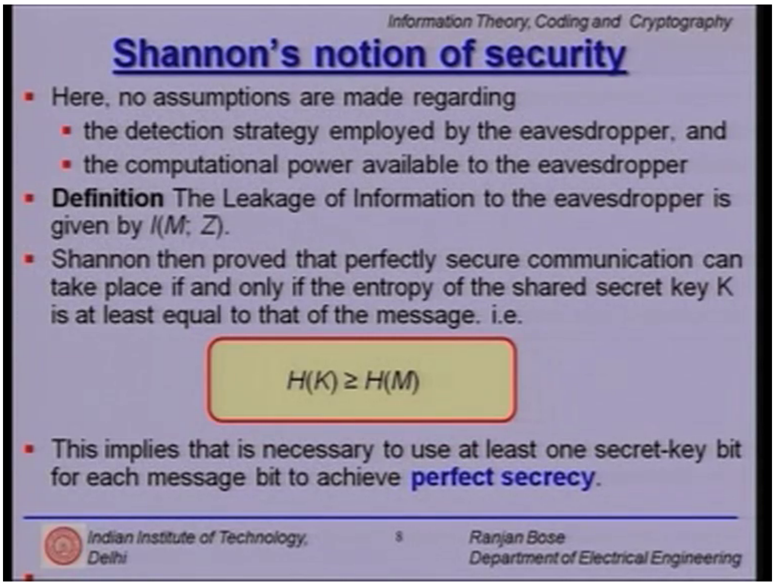
Shannon's cipher model

- Since the mutual information can be expressed as
- $$I(M; Z) = H(M) - H(M/Z)$$
- we conclude that $I(M; Z) = 0$ for **perfect secrecy**.
- In other words, perfect secrecy is achieved if codewords Z are statistically independent of messages, M.

Indian Institute of Technology, Delhi 7 Ranjan Bose Department of Electrical Engineering

So, let us look at this block diagram. We have a message which is encoded by this encoder using this key K and we obtain Z. This is received by the decoder which has the same knowledge about key K, and it decodes it to give M. The eavesdropper however only has Z as it is input. Now, since the mutual information can be expressed as I M semicolon Z is equal to H M minus H M given Z. We conclude that I M semicolon Z should be equal to 0 for perfect secrecy. In other words perfect secrecy is achieved if code words Z and M are statistically independent.

(Refer Slide Time: 05:11)



Information Theory, Coding and Cryptography

Shannon's notion of security

- Here, no assumptions are made regarding
  - the detection strategy employed by the eavesdropper, and
  - the computational power available to the eavesdropper
- **Definition** The Leakage of Information to the eavesdropper is given by $I(M; Z)$.
- Shannon then proved that perfectly secure communication can take place if and only if the entropy of the shared secret key K is at least equal to that of the message. i.e.

$$H(K) \geq H(M)$$

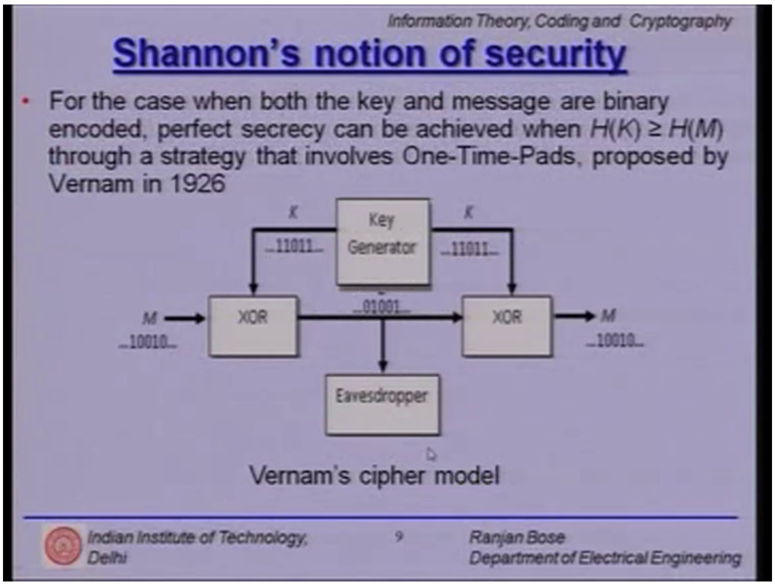
- This implies that is necessary to use at least one secret-key bit for each message bit to achieve **perfect secrecy**.

Indian Institute of Technology, Delhi 8 Ranjan Bose Department of Electrical Engineering

So, Shannon did not assume anything about the deco decoding strategy or the computational power available at the eavesdropper. So, we start with our first definition the leakage of information to the eavesdropper is given by the mutual information I M semicolon Z. Shannon then proved that the perfectly secure communication system can happen if and only if the entropy of the shared key K is at least equal to that of the message that is entropy of key K H of K should be greater than or equal to H of M the entropy of the message.

This implies that is necessary to use at least one secret key bit for every message bit in order to achieve perfect secrecy, which means your key should be equal to even greater than the size of the message M, now is that practical.

(Refer Slide Time: 06:15)



Information Theory, Coding and Cryptography

Shannon's notion of security

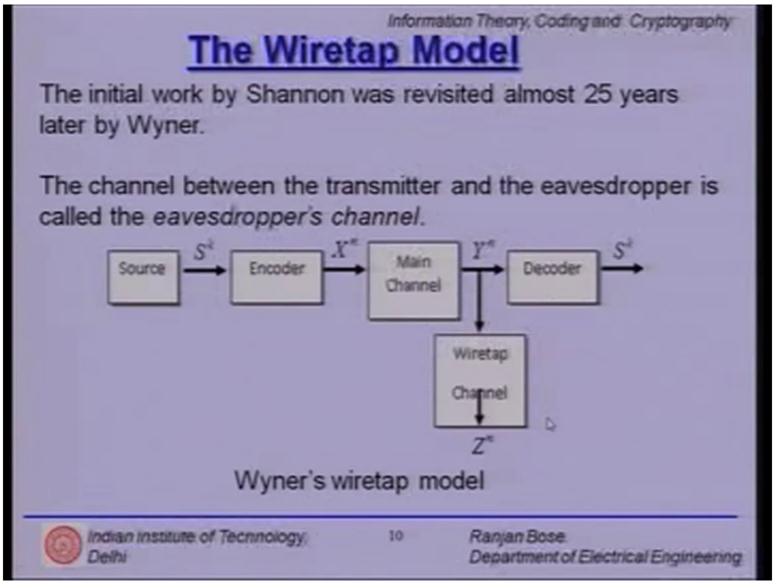
- For the case when both the key and message are binary encoded, perfect secrecy can be achieved when $H(K) \geq H(M)$ through a strategy that involves One-Time-Pads, proposed by Vernam in 1926

Vernam's cipher model

Indian Institute of Technology, Delhi 9 Ranjan Bose Department of Electrical Engineering

So, for the case when both key and message are binary encoded, perfect secrecy can be achieved when H of K is greater than or equal to H of M. And this can be achieved by a strategy called One-Time-Pads, it was first proposed by Vernam in 1926. So, you have a message M binary XORed with key K binary, and then you get encoded message which is binary. It is again XORed back with key K to get back M binary. The eavesdropper has to make do with encrypted message.

(Refer Slide Time: 06:57)



Information Theory, Coding and Cryptography

The Wiretap Model

The initial work by Shannon was revisited almost 25 years later by Wyner.

The channel between the transmitter and the eavesdropper is called the *eavesdropper's channel*.

Source $\xrightarrow{S^k}$ Encoder $\xrightarrow{X^n}$ Main Channel $\xrightarrow{Y^n}$ Decoder $\xrightarrow{\hat{S}^k}$

Wiretap Channel $\rightarrow Z^n$

Wyner's wiretap model

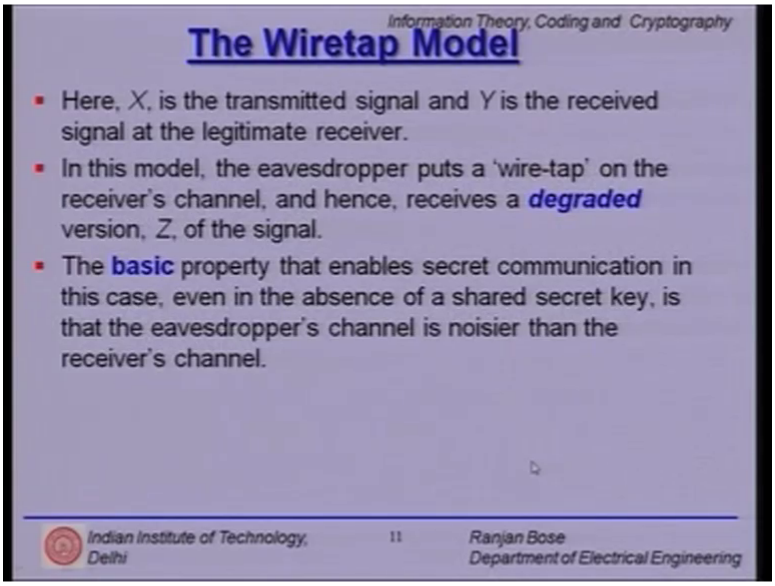
Indian Institute of Technology, Delhi

10

Ranjan Bose
Department of Electrical Engineering

Now, this initial work was exciting, but it was revisited almost 25 years later by Wyner; and he made some improvements. He talked about the wiretap model. So, you have the source. The encoder encodes it to get X of n; and n represents the length of the code in terms of the code word length. It is sent over the main channel which is tapped by the eavesdropper, and he gets Z n. So, clearly the legitimate receiver who is here with the decoder works on Y of n while as the wiretapped channel yields Z of n. So, Y of n is not same as Z of n. This is the wiretap channel.

(Refer Slide Time: 07:48)



Information Theory, Coding and Cryptography

The Wiretap Model

- Here, *X*, is the transmitted signal and *Y* is the received signal at the legitimate receiver.
- In this model, the eavesdropper puts a 'wire-tap' on the receiver's channel, and hence, receives a ***degraded*** version, *Z*, of the signal.
- The **basic** property that enables secret communication in this case, even in the absence of a shared secret key, is that the eavesdropper's channel is noisier than the receiver's channel.

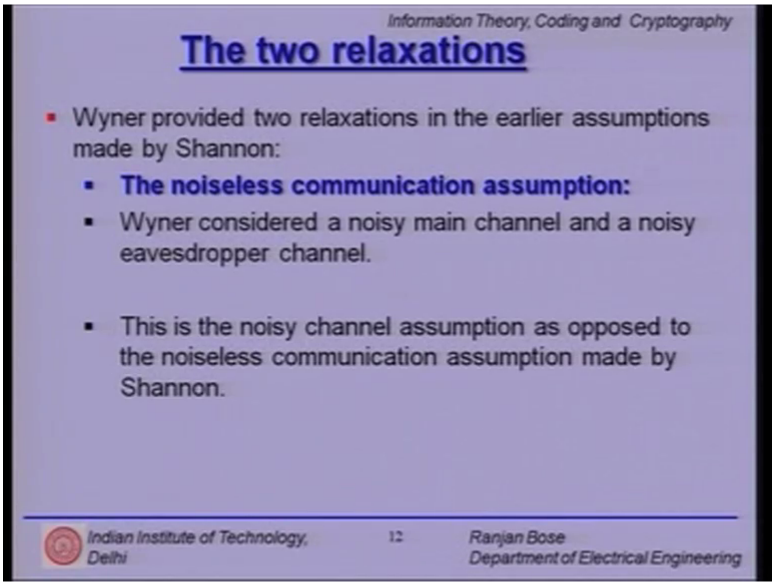
Indian Institute of Technology, Delhi

11

Ranjan Bose
Department of Electrical Engineering

Here, X, is the transmitted signal and Y is the received signal at the legitimate receiver. So, the first assumption is that the wiretap is necessarily a degraded version of the main channel. So, the basic property that enable secret communication in this case even in the absence of a shared secret key is that the eavesdropper's channel is noisier than the receiver's channel.

(Refer Slide Time: 08:14)



Information Theory, Coding and Cryptography

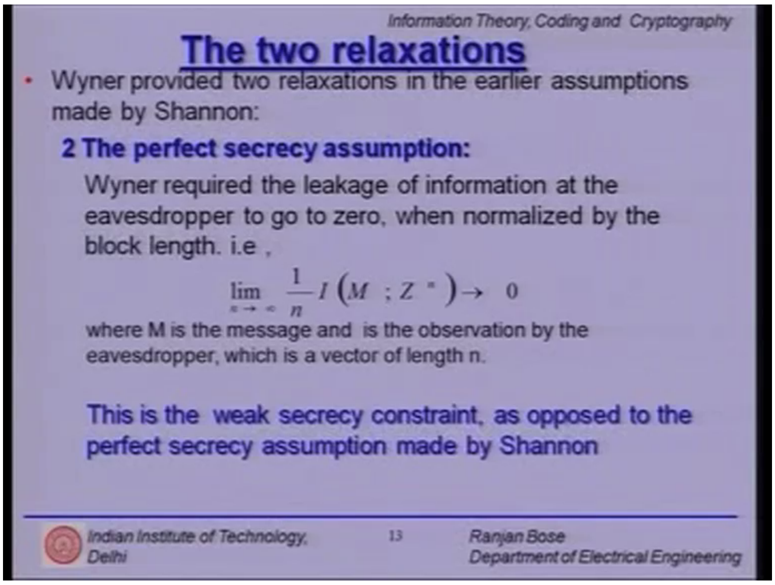
The two relaxations

- Wyner provided two relaxations in the earlier assumptions made by Shannon:
  - **The noiseless communication assumption:**
  - Wyner considered a noisy main channel and a noisy eavesdropper channel.
  - This is the noisy channel assumption as opposed to the noiseless communication assumption made by Shannon.

Indian Institute of Technology, Delhi 12 Ranjan Bose Department of Electrical Engineering

So, Wyner provided two relaxations in the earlier assumptions. First the noiseless communication assumption; So, Wyner considered a noisy main channel and a noisy eavesdropper's channel as opposed to a noiseless main channel and a noiseless eavesdropper's channel by Shannon ok.

(Refer Slide Time: 08:35)



Information Theory, Coding and Cryptography

The two relaxations

- Wyner provided two relaxations in the earlier assumptions made by Shannon:

2 The perfect secrecy assumption:

Wyner required the leakage of information at the eavesdropper to go to zero, when normalized by the block length. i.e ,

$$\lim_{n \to \infty} \frac{1}{n} I\left(M \ ; Z^{n}\right) \to \ 0$$

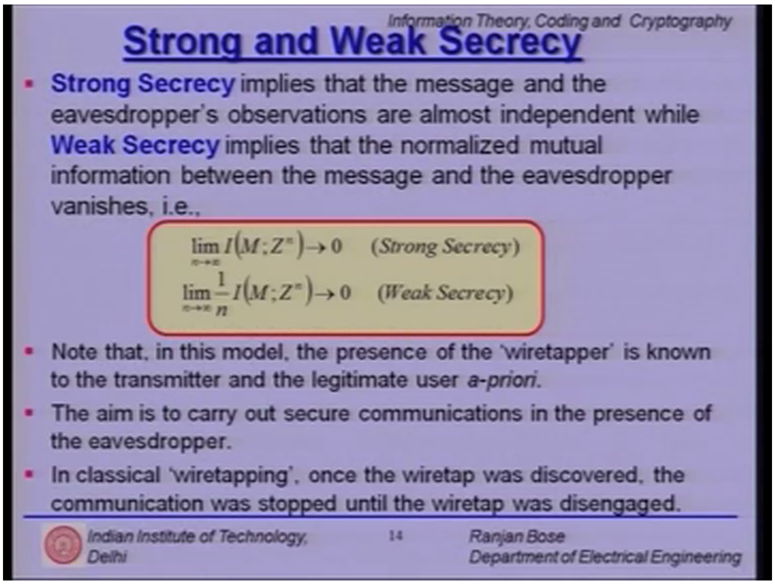
where M is the message and is the observation by the eavesdropper, which is a vector of length n.

This is the weak secrecy constraint, as opposed to the perfect secrecy assumption made by Shannon

Indian Institute of Technology, Delhi 13 Ranjan Bose Department of Electrical Engineering

And relaxation number two the perfect secrecy assumption. What Wyner desired was that the leakage of information at the eavesdropper to go to 0, when normalized by the block length of the code that is limit n tends to infinity, n is the block length of the code normalization factor 1 over n mutual information I between M and Z n the observation of the eavesdropper should tends to 0 as n tends to infinity. This is the weak secrecy constraint. So, we have the second assumption where the perfect security assumption has been relaxed. And the weak secrecy constraint is slightly weaker than the perfect secrecy assumption made by Shannon.

(Refer Slide Time: 09:24)



Information Theory, Coding and Cryptography

Strong and Weak Secrecy

- **Strong Secrecy** implies that the message and the eavesdropper's observations are almost independent while **Weak Secrecy** implies that the normalized mutual information between the message and the eavesdropper vanishes, i.e.,

$$\lim_{n \to \infty} I\left(M ; Z^{n}\right) \to 0 \quad (\textit{Strong Secrecy})$$

$$\lim_{n \to \infty} \frac{1}{n} I\left(M ; Z^{n}\right) \to 0 \quad (\textit{Weak Secrecy})$$

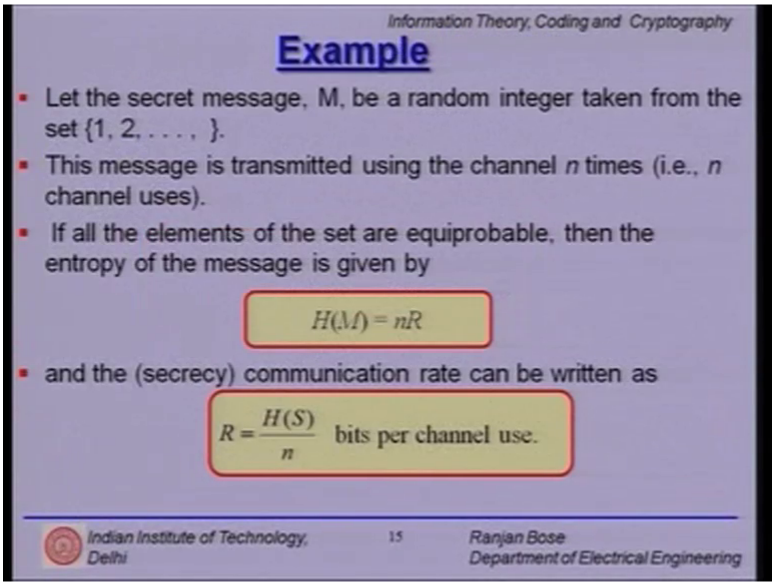
- Note that, in this model, the presence of the 'wiretapper' is known to the transmitter and the legitimate user *a-priori*.
- The aim is to carry out secure communications in the presence of the eavesdropper.
- In classical 'wiretapping', once the wiretap was discovered, the communication was stopped until the wiretap was disengaged.

Indian Institute of Technology, Delhi 14 Ranjan Bose Department of Electrical Engineering

So, what are these strong and weak secrecy notions. Strong Secrecy implies that the message and the eavesdropper observations are almost independent, while weak secrecy implies that the normalized mutual information between the message and eavesdropper vanishes. So, the strong secrecy it is not normalized by 1 over n and weak secrecy is normalized by the block length.

Note that in this model the presence of the 'wiretapper' is known to the transmitter and legitimate user. The idea is to career secure communications even in the presence of the eavesdropper. In classical 'wiretapping' as soon as the wiretapper has discovered you would discontinue communication until the wiretapper disengaged. This is not the case we cannot wait forever we will carry out communication even in the presence of the eavesdropper.

(Refer Slide Time: 10:21)



Information Theory, Coding and Cryptography

Example

- Let the secret message, M, be a random integer taken from the set {1, 2, . . . , }.
- This message is transmitted using the channel n times (i.e., n channel uses).
- If all the elements of the set are equiprobable, then the entropy of the message is given by

$$\boxed{H(M) = nR}$$

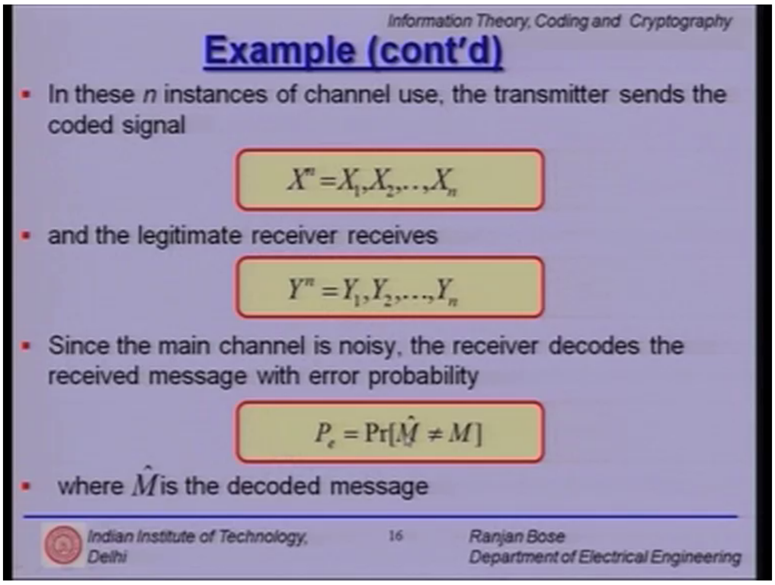
- and the (secrecy) communication rate can be written as

$$\boxed{R = \frac{H(S)}{n} \text{ bits per channel use.}}$$

Indian Institute of Technology, Delhi 15 Ranjan Bose Department of Electrical Engineering

Let us start with the quick example. Let the secret message M be a random integer taken from a set of 1, 2 dot dot dot dot dot. This message is transmitted using the channel n times, so we are looking at n channel users. Now if all the elements of the set are equiprobable then the entropy of the messages simply given by H of M is equal to n R. And the secrecy communication rate can be written as R is equal to H of S normalized by n bits per channel use.

(Refer Slide Time: 10:55)



Information Theory, Coding and Cryptography

Example (cont'd)

- In these n instances of channel use, the transmitter sends the coded signal

$$X^n = X_1, X_2, \ldots, X_n$$

- and the legitimate receiver receives

$$Y^n = Y_1, Y_2, \ldots, Y_n$$

- Since the main channel is noisy, the receiver decodes the received message with error probability

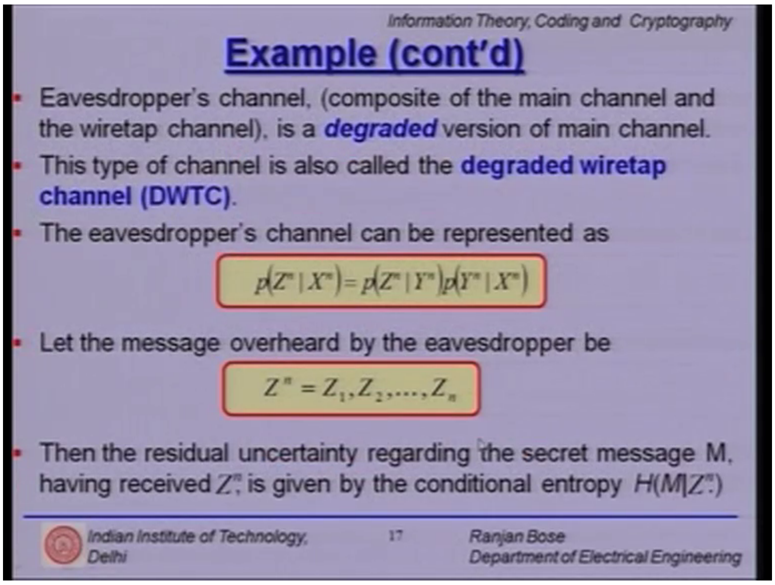
$$P_e = \Pr[\hat{M} \neq M]$$

- where $\hat{M}$ is the decoded message

Indian Institute of Technology, Delhi 16 Ranjan Bose Department of Electrical Engineering

So, in these n instances of channel use, the transmitter sends a coded signal X n as X 1, X 2 up to X n, what the legitimate receiver receives is slightly different from X 1, X 2 to X n because it is a noisy channel. So, the receiver receives Y n as Y 1, Y 2 up to Y n. So, since the main channel is noisy the receiver decodes the receive message with some error probability P e, where message which is decoded which not the same as message being sent.

(Refer Slide Time: 11:26)



Information Theory, Coding and Cryptography

Example (cont'd)

- Eavesdropper's channel, (composite of the main channel and the wiretap channel), is a ***degraded*** version of main channel.
- This type of channel is also called the **degraded wiretap channel (DWTC)**.
- The eavesdropper's channel can be represented as

$$p(Z^n \mid X^n) = p(Z^n \mid Y^n) p(Y^n \mid X^n)$$

- Let the message overheard by the eavesdropper be

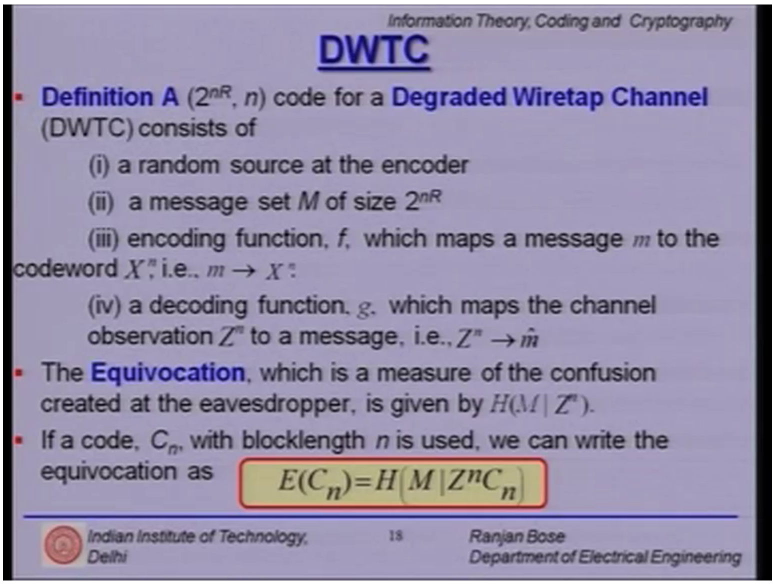
$$Z^n = Z_1, Z_2, \ldots, Z_n$$

- Then the residual uncertainty regarding the secret message M, having received Z^n is given by the conditional entropy $H(M|Z^n)$

Indian Institute of Technology, Delhi 17 Ranjan Bose Department of Electrical Engineering

Now, the eavesdropper’s channel is a degraded version of the main channel. This is the assumption of the degraded wiretapped channel, we call it DWTC. The eavesdropper’s channel can be represented as follows it is the transition probability matrix p Z n given X n is nothing but the product of p Z n given Y n into p Y n given X n. And we have stated earlier that the message over heard by the eavesdropper is Z n; Z 1, Z 2 up to Z n. Then the residual uncertainty regarding the message M, having received Z n is simply given by the conditional entropy H M given Z n.

(Refer Slide Time: 12:09)



Information Theory, Coding and Cryptography

DWTC

- **Definition A** (2^{nR}, n) code for a **Degraded Wiretap Channel** (DWTC) consists of

  (i) a random source at the encoder

  (ii) a message set M of size 2^{nR}

  (iii) encoding function, f, which maps a message m to the codeword X^n; i.e., $m \rightarrow X^n$;

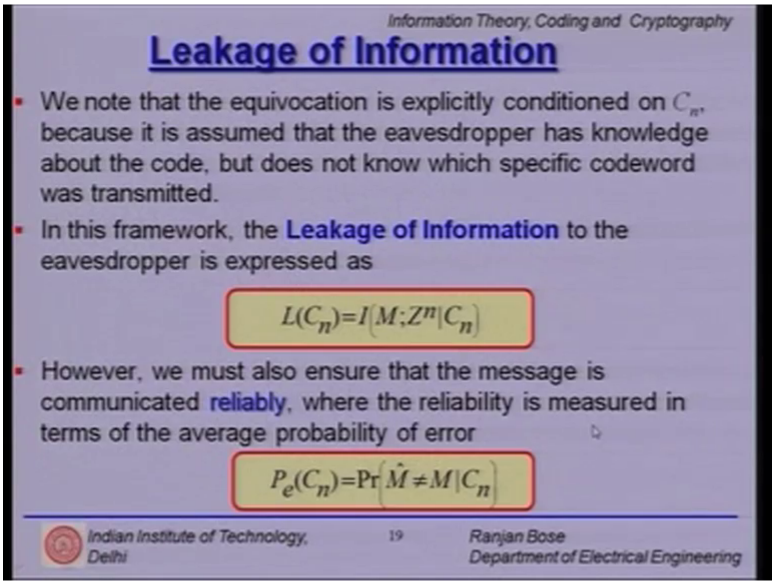
  (iv) a decoding function, g, which maps the channel observation Z^n to a message, i.e., $Z^n \rightarrow \hat{m}$
- The **Equivocation**, which is a measure of the confusion created at the eavesdropper, is given by $H(M \mid Z^n)$.
- If a code, C_n, with blocklength n is used, we can write the equivocation as $\boxed{E(C_n)=H(M|Z^nC_n)}$

Indian Institute of Technology, Delhi 18 Ranjan Bose Department of Electrical Engineering

So, let us talk about the Degraded Wiretap Channel. It consists of a random source at the encoder. A message set M of the size 2 raise to the power n R. And encoding function f which maps the message to the code words. So, this is important. Then coding function is a part of the definition of the degraded wiretap channel. And of course, we need a decoding function at the legitimate receiver which maps the channel observation back to m.

Now, we introduce the notion of Equivocation, which is a measure of the confusion created at the eavesdropper; it is given by H M given Z n. So, if the code C n with block length n is used we can define the equivocation as E of C n equivocation equal to the H entropy of M message given Z n and C n. So, C n also used as a condition.

(Refer Slide Time: 13:19)



Information Theory, Coding and Cryptography

Leakage of Information

- We note that the equivocation is explicitly conditioned on C_n, because it is assumed that the eavesdropper has knowledge about the code, but does not know which specific codeword was transmitted.
- In this framework, the **Leakage of Information** to the eavesdropper is expressed as

$$L(C_n)=I(M;Z^n|C_n)$$

- However, we must also ensure that the message is communicated **reliably**, where the reliability is measured in terms of the average probability of error

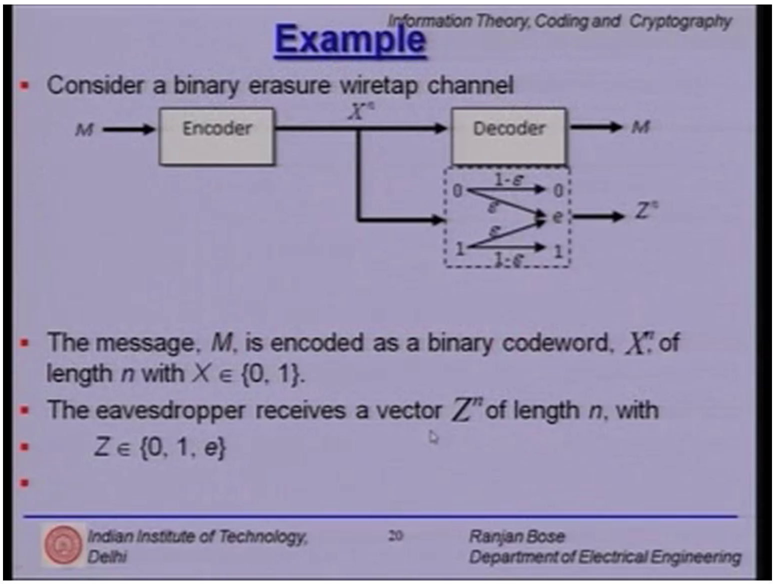
$$P_e(C_n)=\Pr(\hat{M}\neq M|C_n)$$

Indian Institute of Technology, Delhi
19
Ranjan Bose
Department of Electrical Engineering

So, please note equivocation is explicitly conditioned on C n, because it is assumed that the eavesdropper has complete knowledge about the code. What he does not know is which specific code word was transmitted that is where the confusion is in this framework the leakage of information to the eavesdropper is expressed as L leakage of course is the function of the code used is nothing but the mutual information I between M and Z n conditioned on C n.

But please note we must also ensure that the message is communicated reliably, because we are working over the noisy channels. The reliability is measure in terms of the average probability of error P e; again this is the function of the code used.

(Refer Slide Time: 14:10)



Information Theory, Coding and Cryptography

Example

- Consider a binary erasure wiretap channel

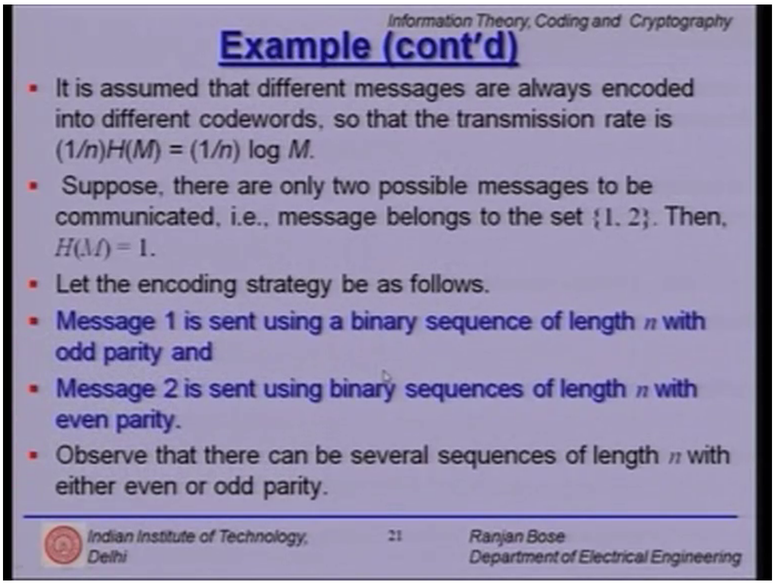
M
Encoder
X^n
Decoder
M
0
1-ε
0
ε
e
ε
1
1-ε
1
Z^n

- The message, M, is encoded as a binary codeword, X_1^n of length n with $X \in \{0, 1\}$.
- The eavesdropper receives a vector Z^n of length n, with
- $Z \in \{0, 1, e\}$
-

Indian Institute of Technology, Delhi 20 Ranjan Bose Department of Electrical Engineering

Now, let us look at an example of a degraded wiretap channel. So, we have the message M encoder gives X m goes to the legitimate receiver he uses the decoder to get back M. Basically M hat. But my friend eavesdropper taps n, but his tap channel is a binary erasure channel. So, 0 codes usually as a 0 but occasionally it ends up as an erasure bit one goes as one, but once in a while turns up at the erasure bit. So, this channel never makes a mistake; it never flips a 0 to 1 or a 1 to 0, but once in a while we get erasure ok.

(Refer Slide Time: 15:01)



Information Theory, Coding and Cryptography

Example (cont'd)

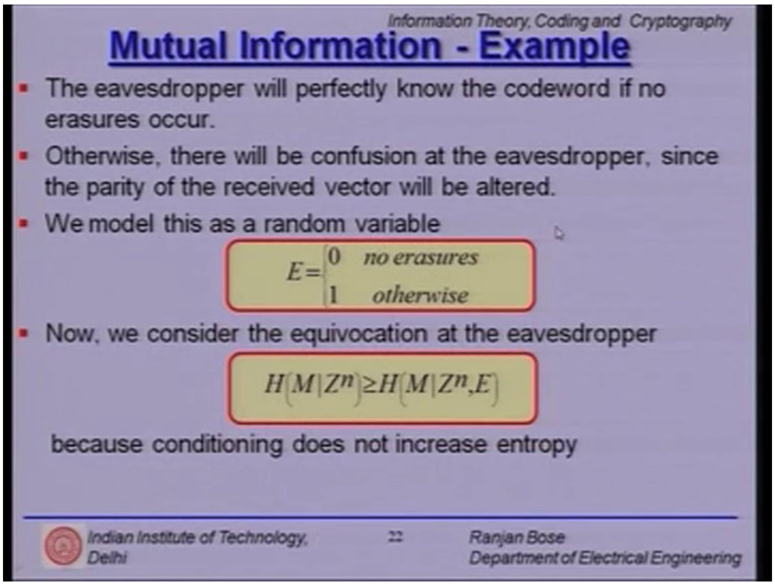
- It is assumed that different messages are always encoded into different codewords, so that the transmission rate is $(1/n)H(M) = (1/n) \log M$.
- Suppose, there are only two possible messages to be communicated, i.e., message belongs to the set $\{1, 2\}$. Then, $H(M) = 1$.
- Let the encoding strategy be as follows.
- Message 1 is sent using a binary sequence of length n with odd parity and
- Message 2 is sent using binary sequences of length n with even parity.
- Observe that there can be several sequences of length n with either even or odd parity.

Indian Institute of Technology, Delhi 21 Ranjan Bose Department of Electrical Engineering

So, it is assumed that different messages are always encoded with different code words, so that the transmission rate is 1 over n H M, which is nothing but 1 over n log M because all messages are equiprobable suppose there are only two possible messages just for the sake of elastration and they belong to the set 1 and 2 then H of M is 1. So, we had pointed out earlier that the encoding strategy forms a part of the definition of the dictated wireless channel.

So, here is r encoding strategy for this example message 1 is sent using a binary sequence of length n with odd parity and message 2 is sent using a binary sequence of length n with even parity. Observe that there can be several sequences of length n with either even or odd parity and this is where the confusion arises.

(Refer Slide Time: 15:56)



Information Theory, Coding and Cryptography

Mutual Information - Example

- The eavesdropper will perfectly know the codeword if no erasures occur.
- Otherwise, there will be confusion at the eavesdropper, since the parity of the received vector will be altered.
- We model this as a random variable

$$E = \begin{cases} 0 & \textit{no erasures} \\ 1 & \textit{otherwise} \end{cases}$$

- Now, we consider the equivocation at the eavesdropper

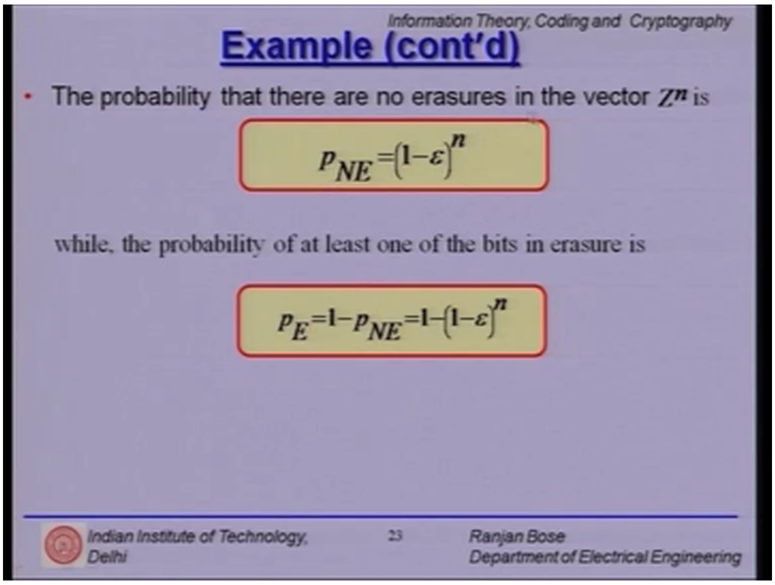
$$H(M|Z^n) \geq H(M|Z^n, E)$$

because conditioning does not increase entropy

Indian Institute of Technology, Delhi 22 Ranjan Bose Department of Electrical Engineering

So, the eavesdropper will perfectly know the code word if no erasures occur otherwise there will be confusion at the eavesdropper since the parity of the received vector will be altered. So, let us model a random variable e equal to 0 if two erasures occur and 1 otherwise. So, let us talk about the equivocation at the eavesdropper H of M given is observations Z of n is now greater than or equal to H of M given Z n comma E because conditioning does not increase entropy.

(Refer Slide Time: 16:33)



Information Theory, Coding and Cryptography

Example (cont'd)

- The probability that there are no erasures in the vector Z^n is

$$p_{NE} = (1-\varepsilon)^n$$

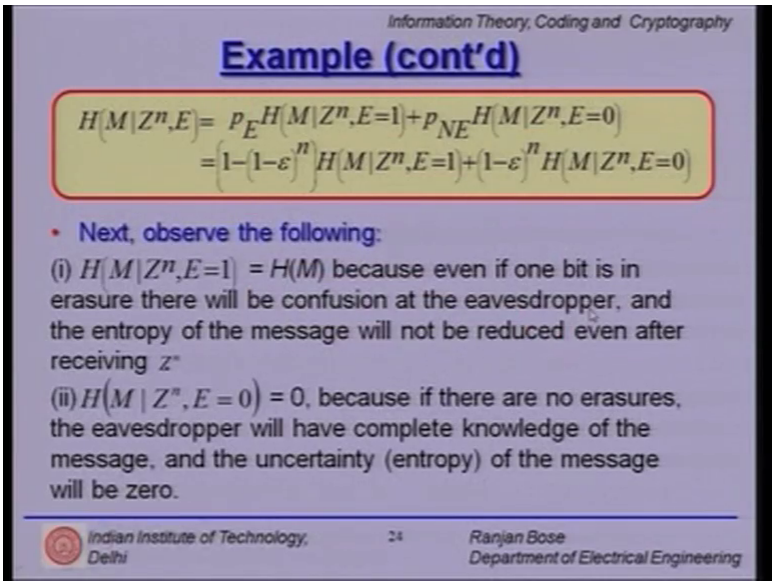
while, the probability of at least one of the bits in erasure is

$$p_E = 1 - p_{NE} = 1-(1-\varepsilon)^n$$

Indian Institute of Technology, Delhi 23 Ranjan Bose Department of Electrical Engineering

So, the probability that there are no erasures in the vectors Z n is simply 1 minus epsilon probability of no erasure all are independent, so raise to the power n and the probability that at least one bit in erasure is 1 minus p N E is this 1 minus bracket open 1 minus epsilon raise to the power n.

(Refer Slide Time: 16:55)



Information Theory, Coding and Cryptography

Example (cont'd)

$$\begin{aligned} H(M|Z^n,E) &= p_E H(M|Z^n,E=1) + p_{NE} H(M|Z^n,E=0) \\ &= \left(1-(1-\varepsilon)^n\right) H(M|Z^n,E=1) + (1-\varepsilon)^n H(M|Z^n,E=0) \end{aligned}$$

- Next, observe the following:

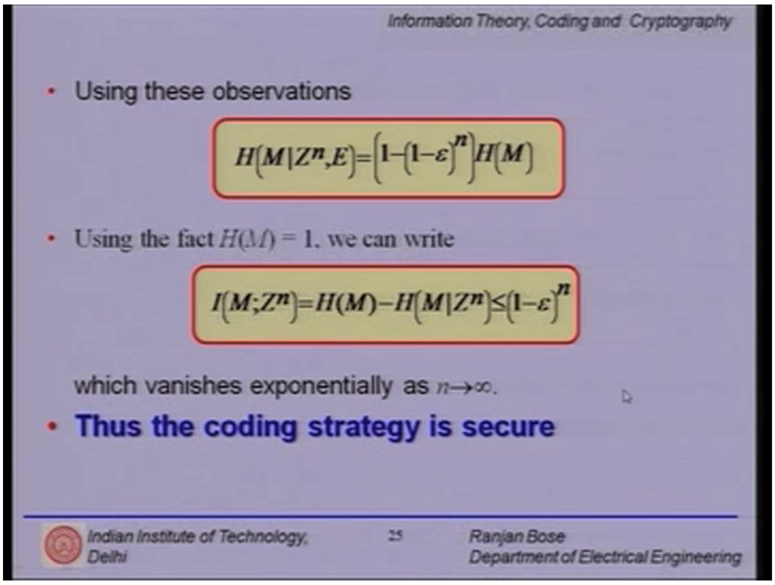
(i) $H(M|Z^n,E=1)$ = $H(M)$ because even if one bit is in erasure there will be confusion at the eavesdropper, and the entropy of the message will not be reduced even after receiving Z^n

(ii) $H(M \mid Z^n, E=0)$ = 0, because if there are no erasures, the eavesdropper will have complete knowledge of the message, and the uncertainty (entropy) of the message will be zero.

Indian Institute of Technology, Delhi 24 Ranjan Bose Department of Electrical Engineering

So, we now look at the equivocation H M given Z n comma E is weighted with the p E and p N E and it is calculated as follows. Now, we observation that H of M given Z n when the case when erasure occurs is M, because even if one bit is erased there will be confusion at the eavesdropper, and the entropy of the message will not be reduced on the other hand for E is equal to 0 when there are no erasures, then the eavesdropper will have complete knowledge about the message because 0 always goes as a 0 and 1 always goes as a 1 in a binaracy erasure channel unless there is an a erasure.

(Refer Slide Time: 16:43)



Information Theory, Coding and Cryptography

- Using these observations

$$\boxed{H(M|Z^n,E)=\left(1-(1-\varepsilon)^n\right)H(M)}$$

- Using the fact $H(M)=1$, we can write

$$\boxed{I(M;Z^n)=H(M)-H(M|Z^n)\leq(1-\varepsilon)^n}$$

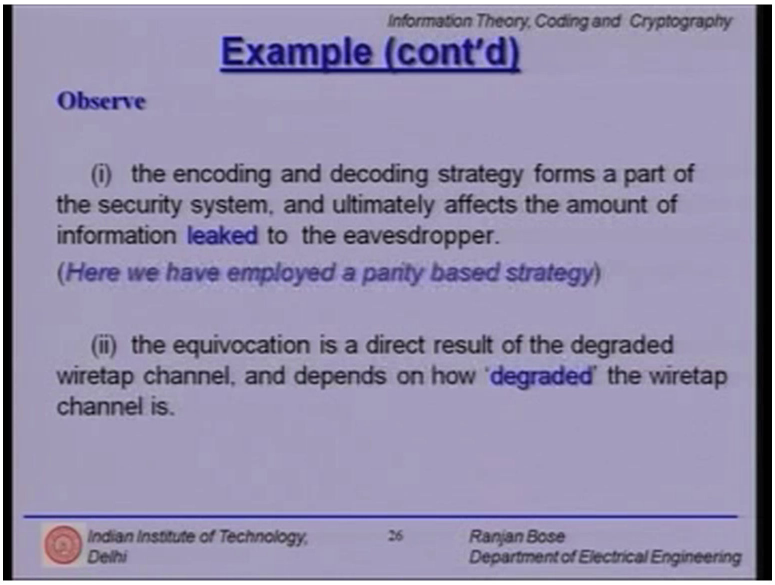
which vanishes exponentially as $n\rightarrow\infty$.

- **Thus the coding strategy is secure**

Indian Institute of Technology, Delhi 25 Ranjan Bose Department of Electrical Engineering

So, using these observations, we can simply write that I M semicolon Z n is nothing but H of M minus H of M given Z n is less than or equal to 1 minus epsilon raise to the power n. Now, what is interesting is epsilon is small, but greater than 0. So, 1 minus epsilon is less than 1 raise to the power n as n tends to infinity it vanishes, so the mutual information between the message and the observation of the eavesdropper vanishes as n tends to infinity does this coding strategy is secure.

(Refer Slide Time: 18:26)



Information Theory, Coding and Cryptography

Example (cont'd)

Observe

(i) the encoding and decoding strategy forms a part of the security system, and ultimately affects the amount of information leaked to the eavesdropper.

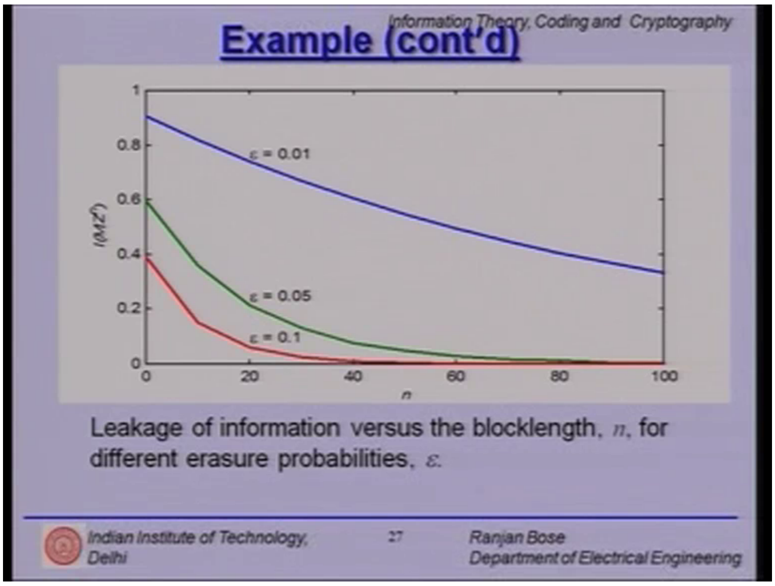
(*Here we have employed a parity based strategy*)

(ii) the equivocation is a direct result of the degraded wiretap channel, and depends on how 'degraded' the wiretap channel is.

Indian Institute of Technology, Delhi 26 Ranjan Bose Department of Electrical Engineering

So, what are the observations the encoding and decoding strategy forms a part of the security system and ultimately affects the amount of information leaked to the eavesdropper. Here we had employed a parity based strategy and it turned out to be secure and the equivocation is a direct result of how degraded the wiretap channel is that is the trick we are playing on.

(Refer Slide Time: 18:54)



Information Theory, Coding and Cryptography

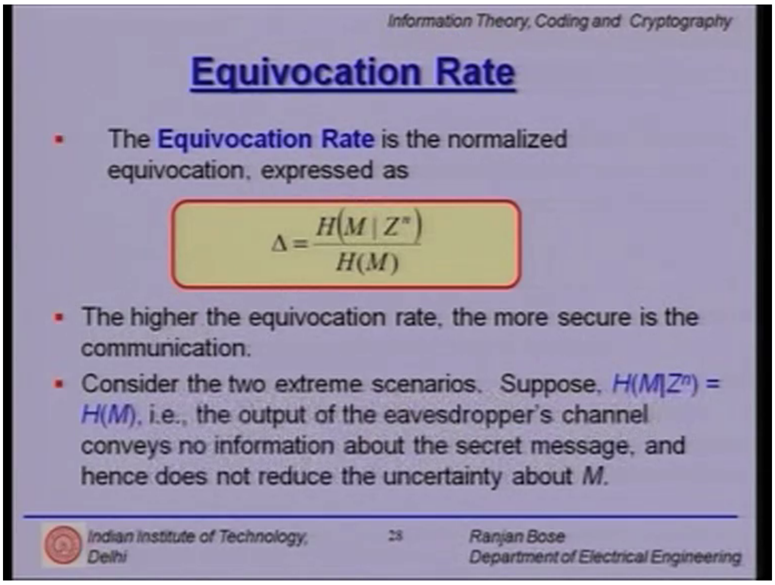
Example (cont'd)

Leakage of information versus the blocklength, n, for different erasure probabilities, ε.

Indian Institute of Technology, Delhi 27 Ranjan Bose Department of Electrical Engineering

So, if you continue the example on the x axis we plot the block length n on the y axis we provide the mutual information I M given I M semicolon Z n, so this is the information leaked to the eavesdropper this is for epsilon is equal to 0.01, so very very low erasure probability fairly good channel, so information leakages high but as soon as the erasure probability increases, the equivocation also increase. So, the poorer channel of the eavesdropper the better is the security of the system this is also highly intitule.

(Refer Slide Time: 19:41)



Information Theory, Coding and Cryptography

Equivocation Rate

- The **Equivocation Rate** is the normalized equivocation, expressed as

$$\boxed{\Delta = \frac{H(M \mid Z^n)}{H(M)}}$$

- The higher the equivocation rate, the more secure is the communication.
- Consider the two extreme scenarios. Suppose, $H(M|Z^n) = H(M)$, i.e., the output of the eavesdropper's channel conveys no information about the secret message, and hence does not reduce the uncertainty about M.

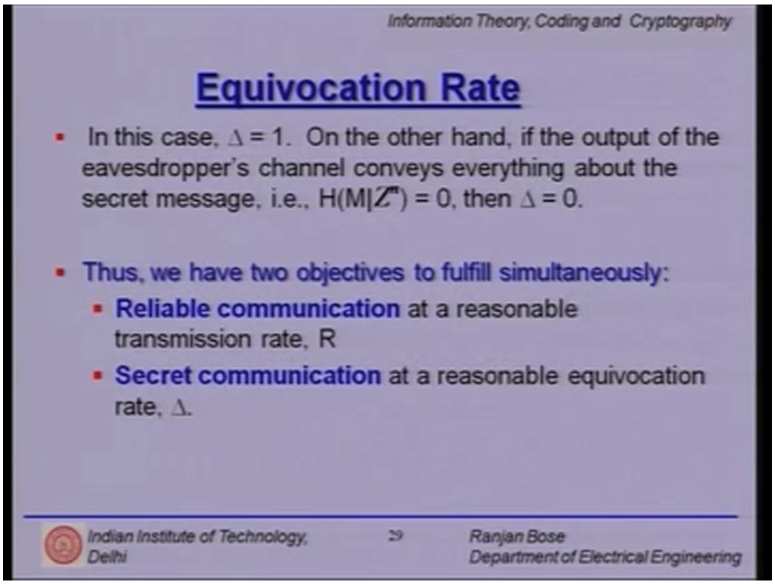
Indian Institute of Technology, Delhi

28

Ranjan Bose
Department of Electrical Engineering

So let us define something called as a equivocation rate. The equivocation rate is the normalized equivocation expressed as delta is equal to H of M given Z n normalized by H of M. So the higher the equivocation rate the more secure is the communication let us consider two extreme scenarios suppose H of M given Z n is H M, that is the output of the eavesdropper's channel conveys absolutely no information about the secret message and hence does not reduce the uncertainty about M.

(Refer Slide Time: 20:22)



Information Theory, Coding and Cryptography

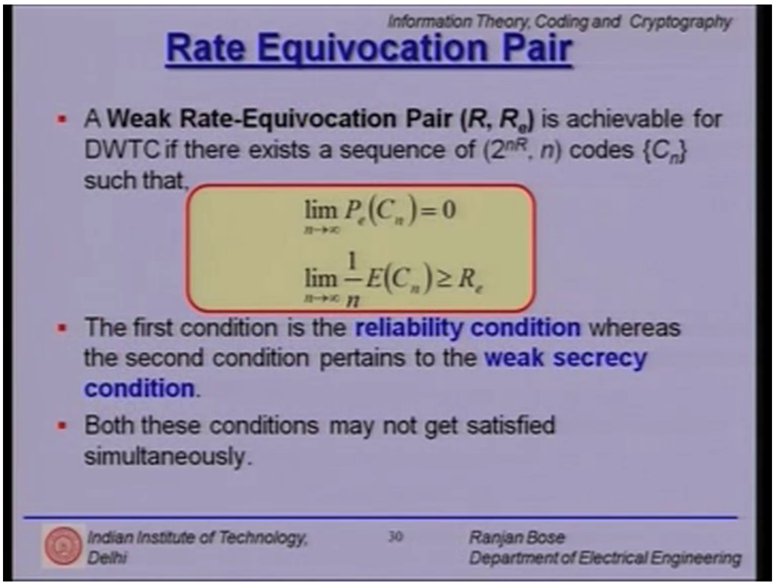
Equivocation Rate

- In this case, $\Delta = 1$. On the other hand, if the output of the eavesdropper's channel conveys everything about the secret message, i.e., $H(M|Z^n) = 0$, then $\Delta = 0$.
- **Thus, we have two objectives to fulfill simultaneously:**
  - **Reliable communication** at a reasonable transmission rate, R
  - **Secret communication** at a reasonable equivocation rate, Δ.

Indian Institute of Technology, Delhi 29 Ranjan Bose Department of Electrical Engineering

In that case, we have delta equal to 1, the other extreme is if the output of the eavesdroppers channel conveys everything about the secret message that is H of M given Z n is 0 then delta is 0, does we have two objectives to fulfill simultaneously number 1 that is about reliability we need to have reliable communication at a reasonable transmission rate R and at the same time secret communication at a reasonable equivocation rate delta. So, transmission rate R and equivocation rate delta, so they form a pair.

(Refer Slide Time: 21:03)



Information Theory, Coding and Cryptography

Rate Equivocation Pair

- A **Weak Rate-Equivocation Pair (R, R_e)** is achievable for DWTC if there exists a sequence of (2^{nR}, n) codes {C_n} such that,

$$\lim_{n\to\infty} P_e(C_n) = 0$$

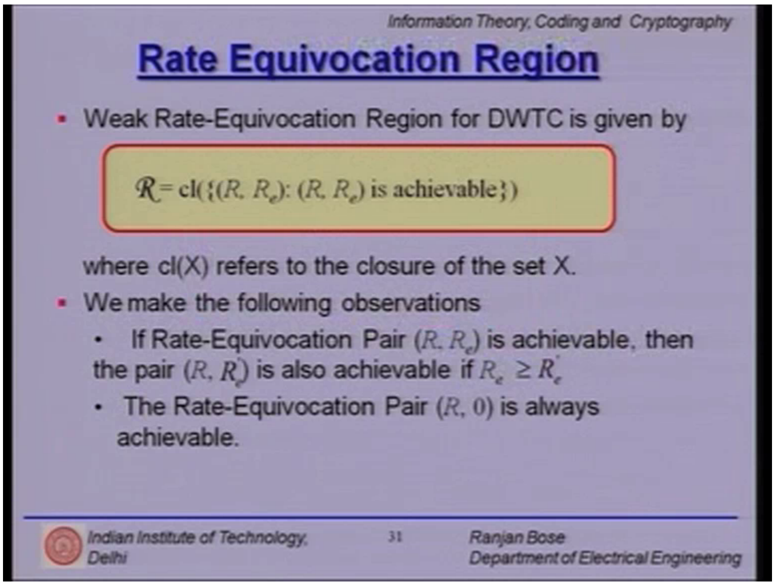
$$\lim_{n\to\infty} \frac{1}{n} E(C_n) \geq R_e$$

- The first condition is the **reliability condition** whereas the second condition pertains to the **weak secrecy condition**.
- Both these conditions may not get satisfied simultaneously.

Indian Institute of Technology, Delhi 30 Ranjan Bose Department of Electrical Engineering

So, let us talk about rate-equivocation pair a weak rate-equivocation pair R comma R sub e is achievable for a degraded wiretap channel if there exists a sequence of 2 raise by n R comma n codes C n such that limit n tends to infinity probability of error C n is equal to 0, the first condition is about the reliability at the same time limit n tends to infinity 1 over n E C n greater than or equal to R e ok. The second conditions pertains to week secrecy condition note both this conditions may not get satisfied simultaneously.

(Refer Slide Time: 21:53)



Information Theory, Coding and Cryptography

Rate Equivocation Region

- Weak Rate-Equivocation Region for DWTC is given by

$$\mathcal{R} = \text{cl}(\{(R, R_e) : (R, R_e) \text{ is achievable}\})$$

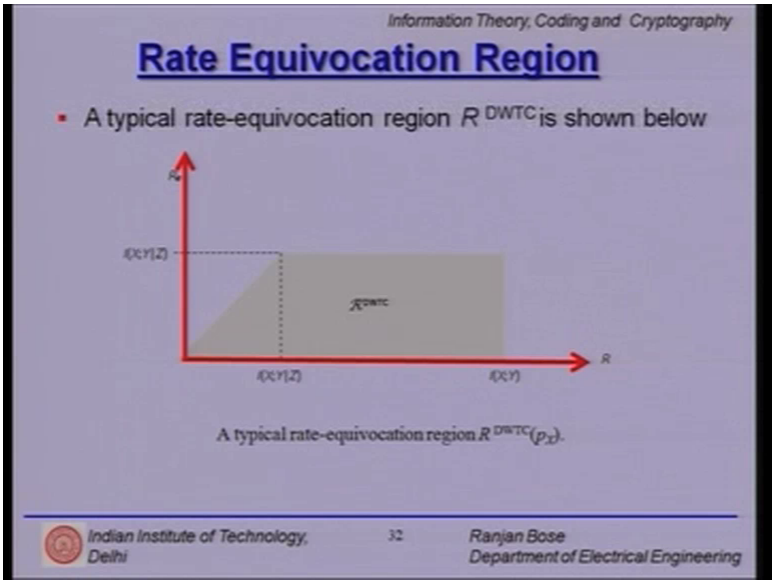
where cl(X) refers to the closure of the set X.

- We make the following observations
  - If Rate-Equivocation Pair (R, R_e) is achievable, then the pair (R, R_e') is also achievable if $R_e \geq R_e'$
  - The Rate-Equivocation Pair $(R, 0)$ is always achievable.

Indian Institute of Technology, Delhi 31 Ranjan Bose Department of Electrical Engineering

We can now start talking about something called as the rate-equivocation region. A weak rate-equivocation region for a degraded wiretap channel is given by R is the closure of the set R comma R sub e where R comma R sub e is achievable. So, we make the following observations if the rate-equivocation pair R comma R sub e is achievable then the pair R comma R sub e prime is also achievable if, R is greater than or equal to R e sub e prime. And the second observation is also very intuitive the rate-equivocation pair R comma 0 is clearly always achievable.

(Refer Slide Time: 22:46)



Information Theory, Coding and Cryptography

Rate Equivocation Region

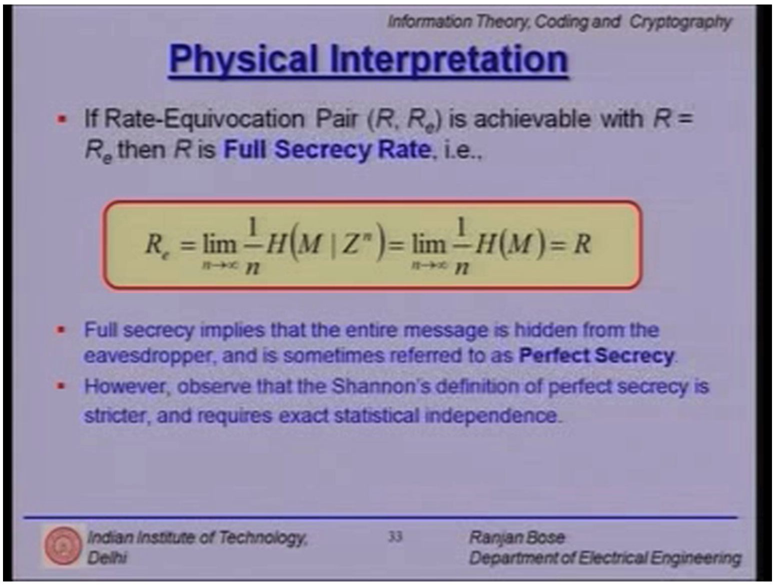
- A typical rate-equivocation region R^{DWTC} is shown below

A typical rate-equivocation region $R^{\mathrm{DWTC}}(p_X)$.

Indian Institute of Technology, Delhi 32 Ranjan Bose Department of Electrical Engineering

What does the typical rate-equivocation region look like here is a plot the x axis is your R the y axis is your R sub e, so we are talking about the information transmission rate and the secrecy rate. And you can have a region where you have the rate-equivocation.

(Refer Slide Time: 23:10)



Information Theory, Coding and Cryptography

Physical Interpretation

- If Rate-Equivocation Pair (R, R_e) is achievable with $R = R_e$ then R is **Full Secrecy Rate**, i.e.,

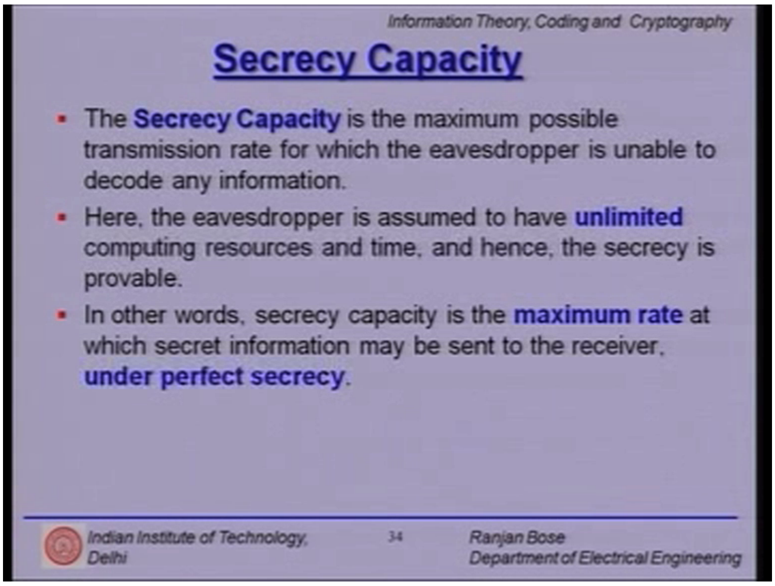
$$\boxed{R_e = \lim_{n\to\infty}\frac{1}{n}H(M \mid Z^n) = \lim_{n\to\infty}\frac{1}{n}H(M) = R}$$

- Full secrecy implies that the entire message is hidden from the eavesdropper, and is sometimes referred to as **Perfect Secrecy**.
- However, observe that the Shannon's definition of perfect secrecy is stricter, and requires exact statistical independence.

Indian Institute of Technology, Delhi 33 Ranjan Bose Department of Electrical Engineering

So, if a rate is equivocation pair R comma R sub e is achievable with R is equal to R e then R is full secrecy rate that is R e is equal to limit n tends to infinity 1 over n H of M given Z n which is a equal to limit n tends to bar over m H of M is equal to R. So, R e equal to R what does it mean, full secrecy implies that the entire message is hidden from the eavesdropper and is also sometimes referred to as perfect secrecy. However, we must note that the Shannon's definition of perfect secrecy is even stricter and requires exact statistical independence, here we have normalized it with respect to n going to infinity.

(Refer Slide Time: 24:04)



Information Theory, Coding and Cryptography

Secrecy Capacity

- The **Secrecy Capacity** is the maximum possible transmission rate for which the eavesdropper is unable to decode any information.
- Here, the eavesdropper is assumed to have **unlimited** computing resources and time, and hence, the secrecy is provable.
- In other words, secrecy capacity is the **maximum rate** at which secret information may be sent to the receiver, **under perfect secrecy**.

Indian Institute of Technology, Delhi

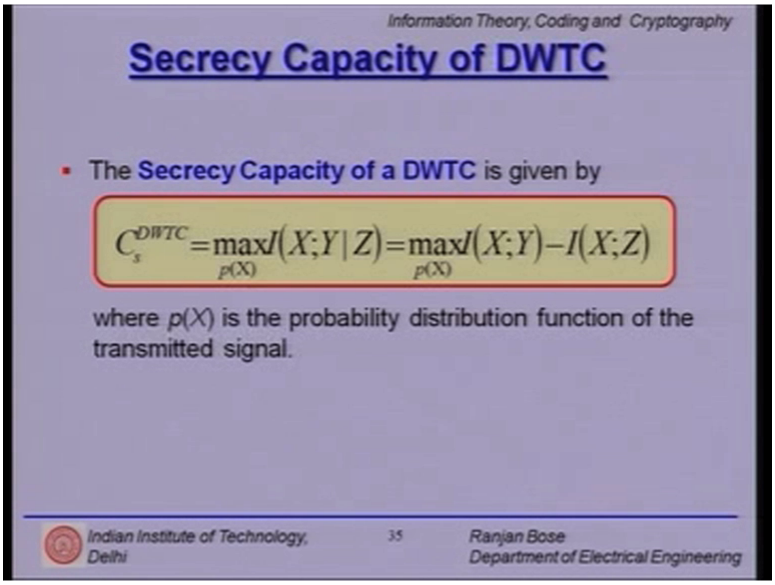
34

Ranjan Bose
Department of Electrical Engineering

Let us now define a very useful quantity called the secrecy capacity. What is secrecy capacity, secrecy capacity is the maximum possible transmission rate for which the eavesdropper is unable to decode any information. Here the eavesdropper is assumed have unlimited computing resources and time resources consequently the secrecy is provable.

So, we cannot make this assumption that the eavesdropper must have only so much time or so much computing resources you can have whatever you want in the world right. So, secrecy capacity is the maximum rate at which secret information may be sent to the receiver under perfect secrecy. This is a very intuitive definition also.

(Refer Slide Time: 24:55)



Information Theory, Coding and Cryptography

Secrecy Capacity of DWTC

- The **Secrecy Capacity of a DWTC** is given by

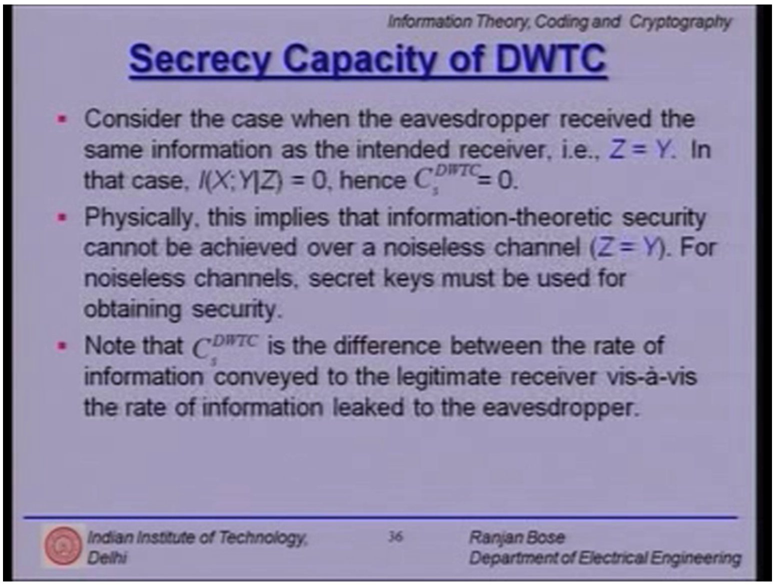
$$\boxed{C_s^{DWTC} = \max_{p(X)} I(X;Y\,|\,Z) = \max_{p(X)} I(X;Y) - I(X;Z)}$$

where $p(X)$ is the probability distribution function of the transmitted signal.

Indian Institute of Technology, Delhi 35 Ranjan Bose Department of Electrical Engineering

So, what is the secrecy capacity of a degraded wiretap channel, it is represented as C sub s for the secrecy capacity of the degraded wiretap channel as the maximum over input probability p of X mutual information I between X semicolon Y given Z. This is nothing but max over p X input probabilities I X semicolon Y minus I X semicolon Z.

(Refer Slide Time: 25:30)



Information Theory, Coding and Cryptography

Secrecy Capacity of DWTC

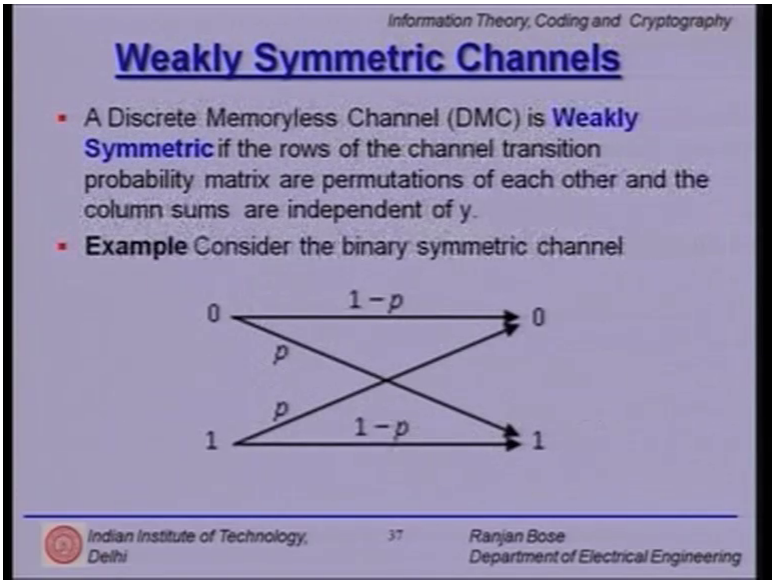
- Consider the case when the eavesdropper received the same information as the intended receiver, i.e., $Z = Y$. In that case, $I(X;Y|Z) = 0$, hence $C_s^{DWTC} = 0$.
- Physically, this implies that information-theoretic security cannot be achieved over a noiseless channel ($Z = Y$). For noiseless channels, secret keys must be used for obtaining security.
- Note that C_s^{DWTC} is the difference between the rate of information conveyed to the legitimate receiver vis-à-vis the rate of information leaked to the eavesdropper.

Indian Institute of Technology, Delhi 36 Ranjan Bose Department of Electrical Engineering

So, consider the case when the eavesdropper received the same information as the intended receiver. So, there is no degradation in the wiretap channel Z is equal to Y in that case I X semicolon Y given Z is 0 and hence, the secrecy capacity is 0. Physically, this implies that the information theoretic security cannot be achieved over a noiseless is eavesdropper’s channel. For noiseless channels secret key must be used for obtaining security. So, our best way it is to have an eavesdroppers channel which is worse of there are main channel.

The other observation is that the secrecy capacity is the difference between the rate of information conveyed to the legitimate receiver vis-a-vis the rate of information leaked to the eavesdropper. So, we are talking about the rate of information send to our desired intended user vis-a-vis what is being leaked and this difference can keep growing as we proceed a long time.

(Refer Slide Time: 26:38)



Information Theory, Coding and Cryptography

Weakly Symmetric Channels

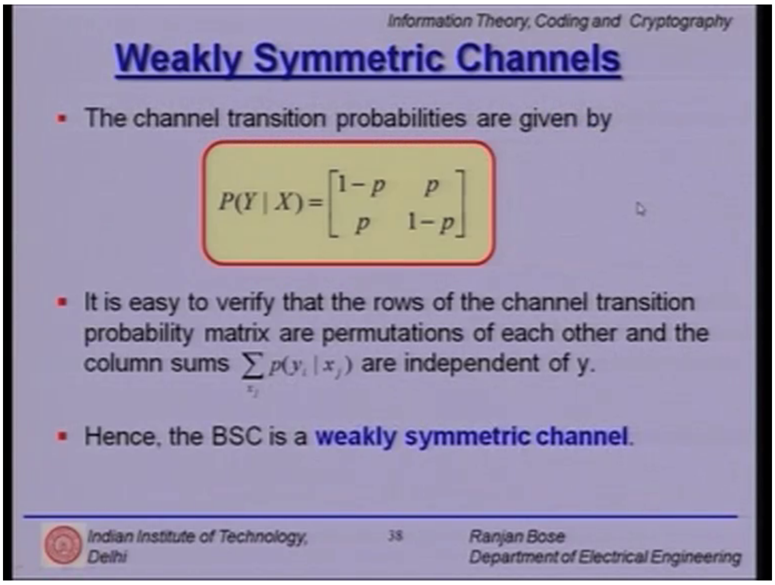
- A Discrete Memoryless Channel (DMC) is **Weakly Symmetric** if the rows of the channel transition probability matrix are permutations of each other and the column sums are independent of y.
- **Example** Consider the binary symmetric channel

0
1 − p
0
p
p
1
1 − p
1

Indian Institute of Technology, Delhi 37 Ranjan Bose Department of Electrical Engineering

Now, let us talk about weekly symmetric channels. A discrete memory less channel is weakly symmetric if the rows of channel transition probability matrix are permutations of each other and the column sums are independent. Our favorite example is the binary symmetric channel shown here.

(Refer Slide Time: 27:04)



Information Theory, Coding and Cryptography

Weakly Symmetric Channels

- The channel transition probabilities are given by

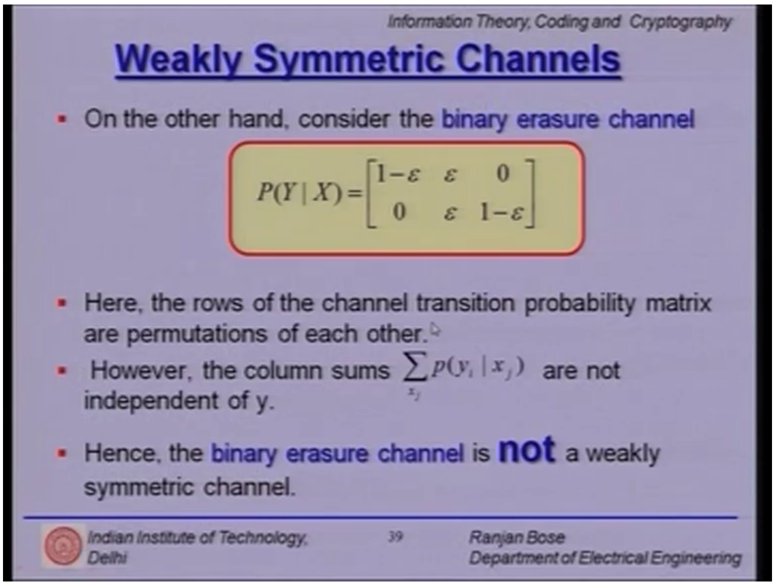
$$P(Y\,|\,X)=\begin{bmatrix}1-p & p\\ p & 1-p\end{bmatrix}$$

- It is easy to verify that the rows of the channel transition probability matrix are permutations of each other and the column sums $\sum_{x_j} p(y_i\,|\,x_j)$ are independent of y.
- Hence, the BSC is a **weakly symmetric channel**.

Indian Institute of Technology, Delhi 38 Ranjan Bose Department of Electrical Engineering

The channel probability channel transition probabilities are given by this matrix for the binary symmetric channel. And it is easy to verify that the rows of the channel transition probabilities matrix are simply the permutations of each other and the column sums are independent of y. Clearly the binary symmetric channel is a weekly symmetric channel.

(Refer Slide Time: 27:26)



Information Theory, Coding and Cryptography

Weakly Symmetric Channels

- On the other hand, consider the binary erasure channel

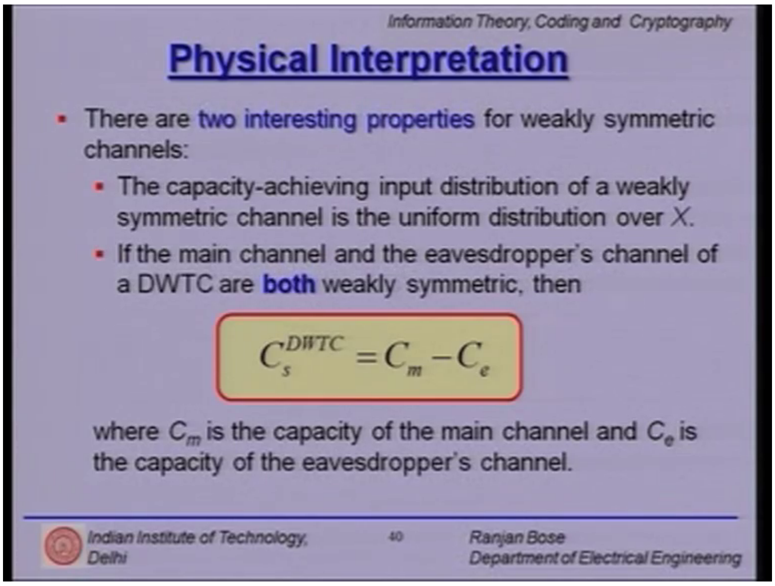
$$P(Y\,|\,X)=\begin{bmatrix}1-\varepsilon & \varepsilon & 0\\ 0 & \varepsilon & 1-\varepsilon\end{bmatrix}$$

- Here, the rows of the channel transition probability matrix are permutations of each other.
- However, the column sums $\sum_{x_j} p(y_i\,|\,x_j)$ are not independent of y.
- Hence, the binary erasure channel is **not** a weakly symmetric channel.

Indian Institute of Technology, Delhi 39 Ranjan Bose Department of Electrical Engineering

On the other hand, our second favorite the binary erasure channel is not weakly symmetric. Here the rows of the channel transition probability matrix are permutations of each other. However, the column sums are clearly not independent of y, so it is not weekly symmetric.

(Refer Slide Time: 27:48)



Information Theory, Coding and Cryptography

Physical Interpretation

- There are two interesting properties for weakly symmetric channels:
  - The capacity-achieving input distribution of a weakly symmetric channel is the uniform distribution over X.
  - If the main channel and the eavesdropper's channel of a DWTC are **both** weakly symmetric, then

$$\boxed{C_s^{DWTC} = C_m - C_e}$$

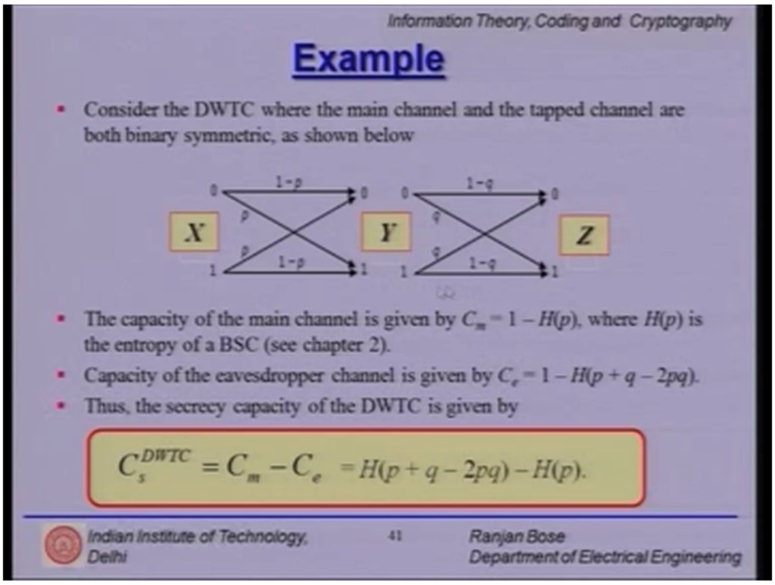
where C_m is the capacity of the main channel and C_e is the capacity of the eavesdropper's channel.

Indian Institute of Technology, Delhi 40 Ranjan Bose Department of Electrical Engineering

So, why are we talking about weekly symmetric channels here. Well, there are two interesting properties is for weekly symmetric channels. First the capacity achieving input distribution of a weekly symmetric channel is simply the uniform distribution over X.

And second if the main channel and the eavesdropper's channel of a degraded wiretap channel are both weekly symmetric, then it is very easy to calculate the secrecy capacity of the degraded wiretap channel. What is it, it is simply difference between the capacity of the main channel C m and the capacity of the eavesdropper's channel C e. Please note the condition is that both the main channel and the eavesdropper's channel are weekly symmetric channels.

(Refer Slide Time: 28:37)


0
1-p
0
p
p
1-p
1
1
X
Y
0
1-q
0
q
q
1-q
1
1
Z

Information Theory, Coding and Cryptography

Example

- Consider the DWTC where the main channel and the tapped channel are both binary symmetric, as shown below
- The capacity of the main channel is given by $C_m = 1 - H(p)$, where $H(p)$ is the entropy of a BSC (see chapter 2).
- Capacity of the eavesdropper channel is given by $C_e = 1 - H(p + q - 2pq)$.
- Thus, the secrecy capacity of the DWTC is given by

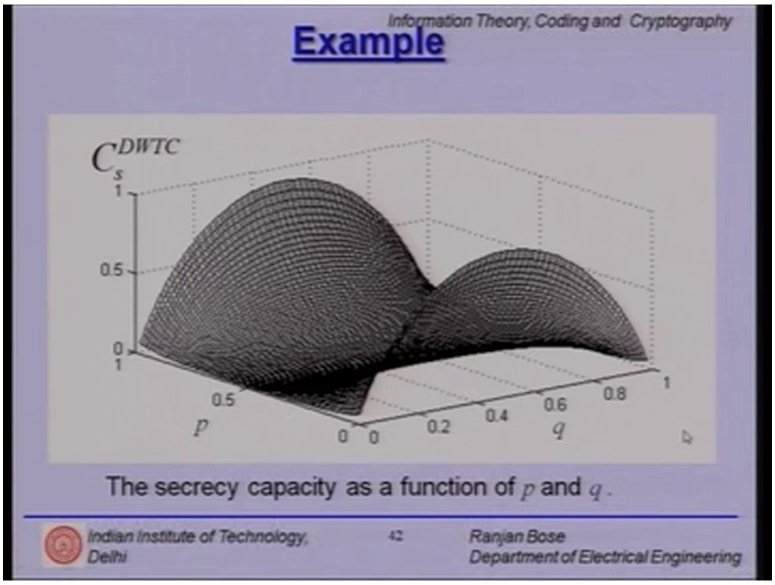
$$\boxed{C_s^{DWTC} = C_m - C_e = H(p + q - 2pq) - H(p).}$$

Indian Institute of Technology, Delhi 41 Ranjan Bose Department of Electrical Engineering

Let us look at an example. My sender X trying to communicate with X the legitimate receiver and somewhere Z has tapped the channel by it is a degraded wiretap channel. So, the composite channel for Z is the concatenation of the main channel and the wiretap channel. But note that the main channel is binary symmetric channel hence weakly symmetric, so is the second wiretap channel.

So the capacity of the eavesdropper's channel is C e capacity of the main channel is C m and C m is nothing but 1 minus H of p where H p is the entropy of the binary symmetric channel we have seen it before. Similarly, C e which is the composite of two binary symmetric channel is also an effective binary symmetric channel is 1 minus H p plus q minus 2 p q. So, the secrecy capacity of this degraded wireless degraded wiretap channel is simply given by C m minus C e is H p plus q minus 2 p q minus H of p, it is very easy to calculate.

(Refer Slide Time: 29:48)



Information Theory, Coding and Cryptography

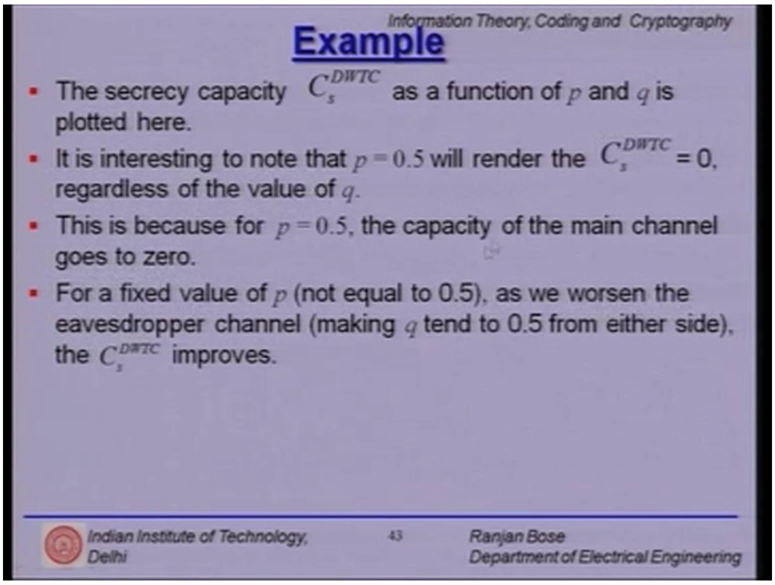
Example

The secrecy capacity as a function of p and q.

Indian Institute of Technology, Delhi 42 Ranjan Bose Department of Electrical Engineering

How does it look? Well, on the x-axis, we have plotted the probabilities of q the wiretap channel; on the y-axis, we have p the probability of error for the main channel; on the z axis, we have the secrecy capacity. Please note whenever p is 0 then the C s is 0 for the main channel is useless then there is no notion of secrecy capacity has been greater than 0. On the other hand, when p is not equal to 0 and when q approaches 0.5 on either side that is it is a poor channel for the wiretap channel, we have higher secrecy capacity.

(Refer Slide Time: 30:35)



Information Theory, Coding and Cryptography

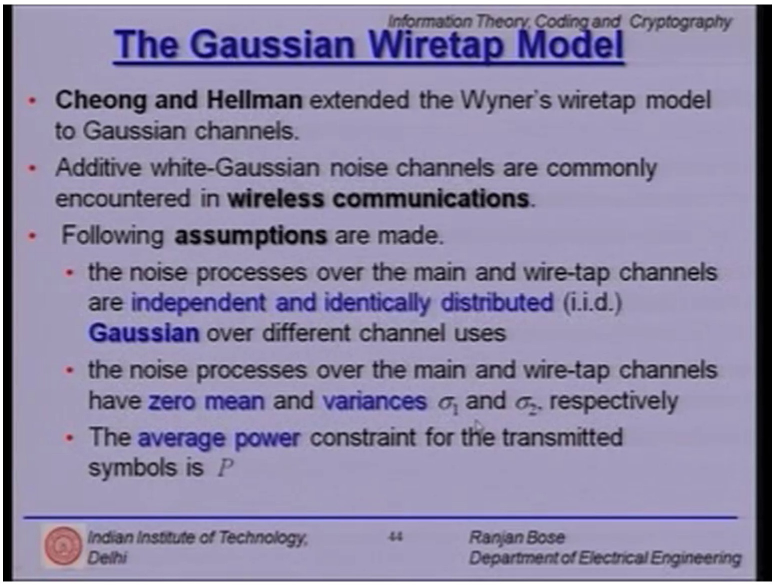
Example

- The secrecy capacity C_s^{DWTC} as a function of p and q is plotted here.
- It is interesting to note that $p = 0.5$ will render the $C_s^{DWTC} = 0$, regardless of the value of q.
- This is because for $p = 0.5$, the capacity of the main channel goes to zero.
- For a fixed value of p (not equal to 0.5), as we worsen the eavesdropper channel (making q tend to 0.5 from either side), the C_s^{DWTC} improves.

Indian Institute of Technology, Delhi 43 Ranjan Bose Department of Electrical Engineering

So, this is summarized in this slide that when p is equal to 0.5, it will render the C s equal to 0 regardless of the value of q.

(Refer Slide Time: 30:49)



Information Theory, Coding and Cryptography

The Gaussian Wiretap Model

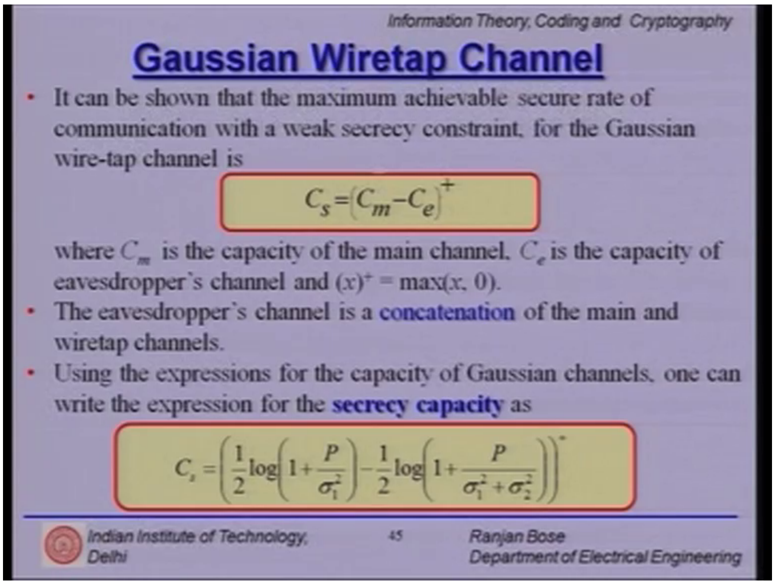
- **Cheong and Hellman** extended the Wyner's wiretap model to Gaussian channels.
- Additive white-Gaussian noise channels are commonly encountered in **wireless communications**.
- Following **assumptions** are made.
  - the noise processes over the main and wire-tap channels are independent and identically distributed (i.i.d.) **Gaussian** over different channel uses
  - the noise processes over the main and wire-tap channels have zero mean and variances σ_1 and σ_2, respectively
  - The average power constraint for the transmitted symbols is P

Indian Institute of Technology, Delhi 44 Ranjan Bose Department of Electrical Engineering

Now, Cheong and Hellman extended Wyner’s wiretap model to Gaussian Channels, because they are also very popular. Additive white-Gaussian noise channel are commonly encountered in wireless communications. And they made the following assumptions.

Number 1, the noise process over the main and wire-tap channels are independent and identically distributed Gaussian over different channel uses. Number 2, the noise processes over the main and wiretap channels have zero mean and variances sigma 1 squared and sigma 2 squared respectively. The average power constraint for the transmitted symbols is P.

(Refer Slide Time: 31:29)



Information Theory, Coding and Cryptography

Gaussian Wiretap Channel

- It can be shown that the maximum achievable secure rate of communication with a weak secrecy constraint, for the Gaussian wire-tap channel is

$$C_s = (C_m - C_e)^+$$

where C_m is the capacity of the main channel, C_e is the capacity of eavesdropper's channel and $(x)^+ = \max(x, 0)$.
- The eavesdropper's channel is a **concatenation** of the main and wiretap channels.
- Using the expressions for the capacity of Gaussian channels, one can write the expression for the **secrecy capacity** as

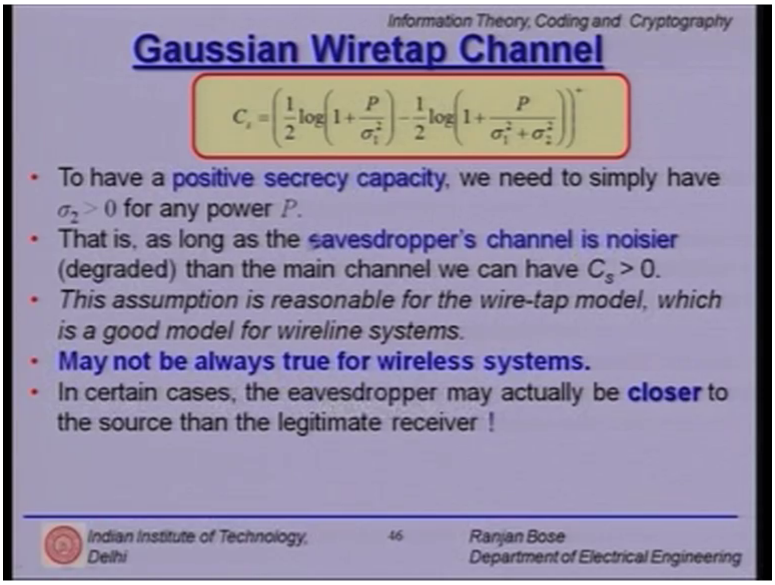
$$C_s = \left(\frac{1}{2}\log\left(1+\frac{P}{\sigma_1^2}\right) - \frac{1}{2}\log\left(1+\frac{P}{\sigma_1^2+\sigma_2^2}\right)\right)^+$$

Indian Institute of Technology, Delhi 45 Ranjan Bose Department of Electrical Engineering

So, let us talk little bit more about this Gaussian wire-tap channel. It can be shown that the maximum achievable secure rate of communication with a weak secrecy constraint for the Gaussian wire-tap channel is C s equal to C m minus C e with a superscript plus sign which is x super plus is nothing but max of x of 0. So, it cannot be negative it can at best b 0 minimum.

So, the eavesdropper’s channel is a concatenation of the main channel and the wiretap channel. But we know the expression for the capacity of the Gaussian channel and if we plug these values n then the capacity of the Gaussian channel. The secrecy capacity can be expressed at C s equal to this is the capacity of the main Gaussian channel and this is the capacity of wiretap channel. Please note since it is a concatenations, it is sigma 1 squared plus sigma 2 squared.

(Refer Slide Time: 32:28)



Information Theory, Coding and Cryptography

Gaussian Wiretap Channel

$$C_s = \left(\frac{1}{2}\log\left(1+\frac{P}{\sigma_1^2}\right) - \frac{1}{2}\log\left(1+\frac{P}{\sigma_1^2+\sigma_2^2}\right)\right)^+$$

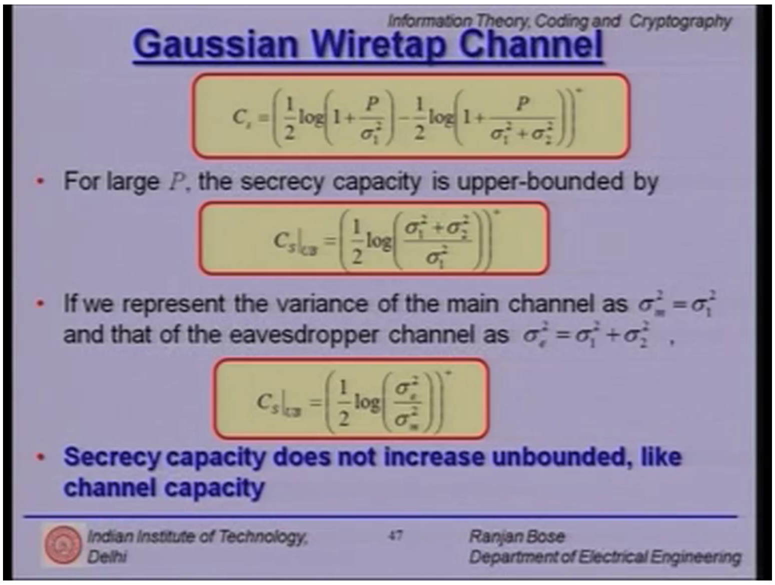
- To have a positive secrecy capacity, we need to simply have $\sigma_2 > 0$ for any power P.
- That is, as long as the eavesdropper's channel is noisier (degraded) than the main channel we can have $C_s > 0$.
- *This assumption is reasonable for the wire-tap model, which is a good model for wireline systems.*
- **May not be always true for wireless systems.**
- In certain cases, the eavesdropper may actually be **closer** to the source than the legitimate receiver !

Indian Institute of Technology, Delhi 46 Ranjan Bose Department of Electrical Engineering

So, just analyzing this expression, we have positive secrecy capacity if sigma 2 squared is greater than 0 for any power P ok. So, we make the second term smaller than the first term and we have a greater than 0 C s. What does it mean, as long as the eavesdropper's channel is noisier that is degraded than the main channel, we have a hope for C s, the secrecy capacity greater than 0.

This is assumption is reasonable for the wire-tap model, which is good for wireless systems. But is it a faire assumption to make for wireless system. I mean in wireless systems eavesdropper can be anywhere in the room, and it could also be closer to the source than the legitimate receiver. Clearly the Gaussian wire-tap channel is interesting academically, but for wireless scenario this may not be a very good assumption in any case let us continue our discussion.

(Refer Slide Time: 33:27)



Information Theory, Coding and Cryptography

Gaussian Wiretap Channel

$$C_s = \left(\frac{1}{2}\log\left(1+\frac{P}{\sigma_1^2}\right) - \frac{1}{2}\log\left(1+\frac{P}{\sigma_1^2+\sigma_2^2}\right)\right)^+$$

- For large P, the secrecy capacity is upper-bounded by

$$C_S\big|_{UB} = \left(\frac{1}{2}\log\left(\frac{\sigma_1^2+\sigma_2^2}{\sigma_1^2}\right)\right)^+$$

- If we represent the variance of the main channel as $\sigma_m^2 = \sigma_1^2$ and that of the eavesdropper channel as $\sigma_e^2 = \sigma_1^2 + \sigma_2^2$,

$$C_S\big|_{UB} = \left(\frac{1}{2}\log\left(\frac{\sigma_e^2}{\sigma_m^2}\right)\right)^+$$

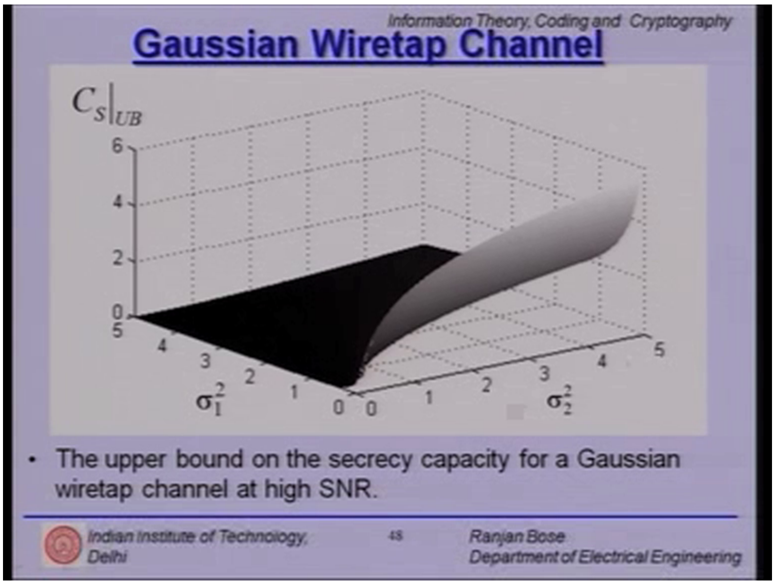
- **Secrecy capacity does not increase unbounded, like channel capacity**

Indian Institute of Technology, Delhi 47 Ranjan Bose Department of Electrical Engineering

So, looking at the expression for the secrecy capacity of the Gaussian wiretap channel, and for large values of P this 1 can be neglected and this simplify into C s upper-bound as follows where clearly the P has disappeared from the equation. So, for high values of P, the secrecy capacity becomes independent of the transmit power P.

If we represent the main channel as sigma m squared the noise power and for the eavesdropper's channel the sum as sigma e squared then C s upper-bound is nothing but half log sigma e squared over sigma m squared. So, what is the take home message here, the secrecy capacity does not increase unbounded like channel capacity ok.

(Refer Slide Time: 34:23)



Information Theory, Coding and Cryptography

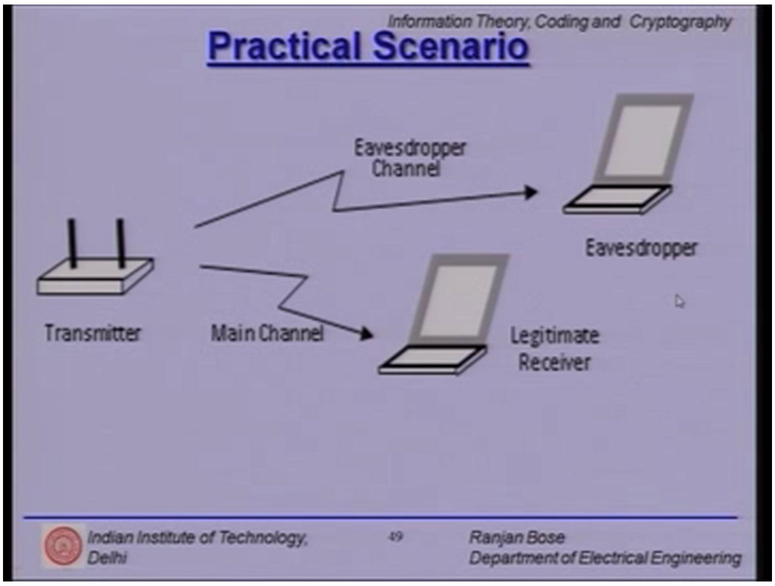
Gaussian Wiretap Channel

- The upper bound on the secrecy capacity for a Gaussian wiretap channel at high SNR.

Indian Institute of Technology, Delhi 48 Ranjan Bose Department of Electrical Engineering

Here is a plot to illustrate the point. On the x-axis, we have sigma 2 squared; on this axis, we have sigma 1 squared; on z axis, we have the upper-bound plotted. And the curve look something like this.

(Refer Slide Time: 34:39)



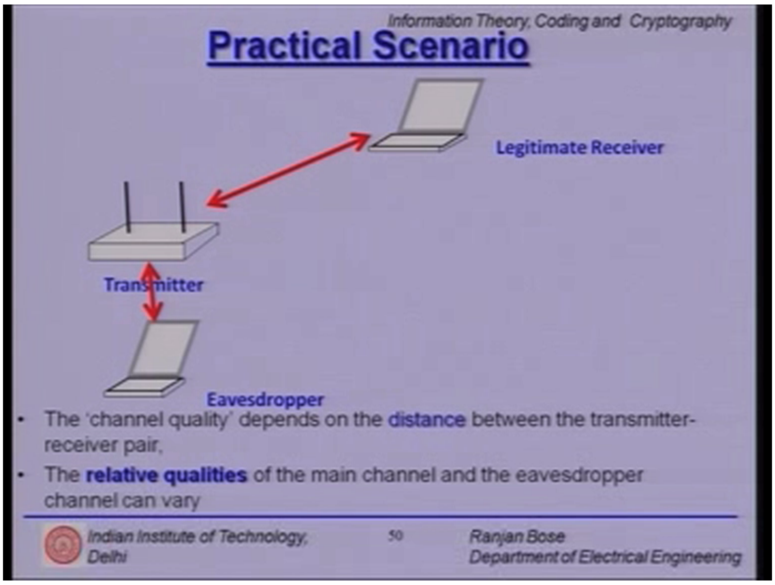
Information Theory, Coding and Cryptography

Practical Scenario

Indian Institute of Technology, Delhi 49 Ranjan Bose Department of Electrical Engineering

Now, let us look at the Practical Scenario. We have a transmitter; we have a receiver it is a wireless channel so it is a main channel here. And clearly there is an eavesdropper where there is a eavesdropper's channel; these are independent and no assumptions are made what is the location of the receiver which is legitimate and the eavesdropper.

(Refer Slide Time: 35:04)



Information Theory, Coding and Cryptography

Practical Scenario

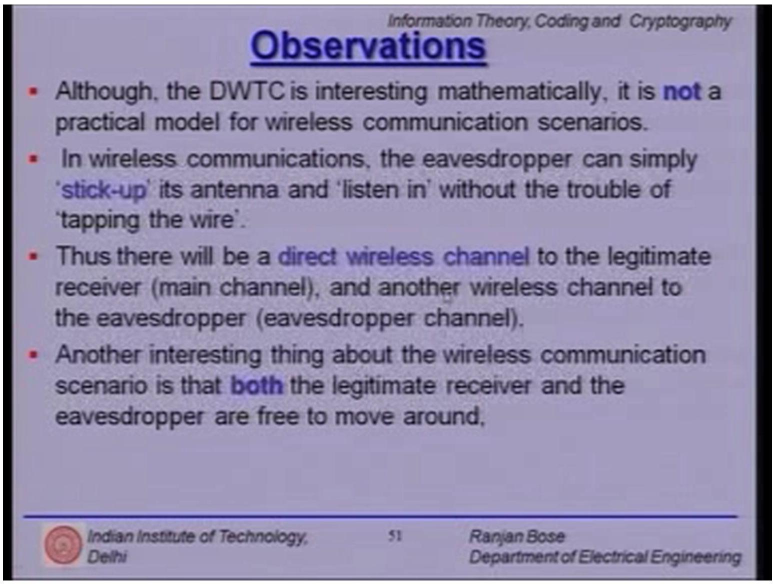
- The 'channel quality' depends on the distance between the transmitter-receiver pair.
- The **relative qualities** of the main channel and the eavesdropper channel can vary

Indian Institute of Technology, Delhi 50 Ranjan Bose Department of Electrical Engineering

So, let us put the transmitter somewhere in the room. And we introduce are front the legitimate receiver who is try to communicate with the transmitter. Now, with or without a knowledge an eavesdropper walks into the room, and it does what it supposed to do eavesdrop on the message is being sent from the transmitter to the receiver. Now, these two the legitimate receiver and the eavesdropper can be located anywhere within the room.

And so happens that it is possible that the eavesdropper could be closer to the transmitter then the legitimate receiver. Now, the channel quality depends on the distance between the transmitter receiver pair. So, in this case, the eavesdropper ends up having a better channel than the legitimate receiver. The relative quantities of and the quality of the main channel and the eavesdropper's channel can vary depending upon the relative locations.

(Refer Slide Time: 36:03)



Information Theory, Coding and Cryptography

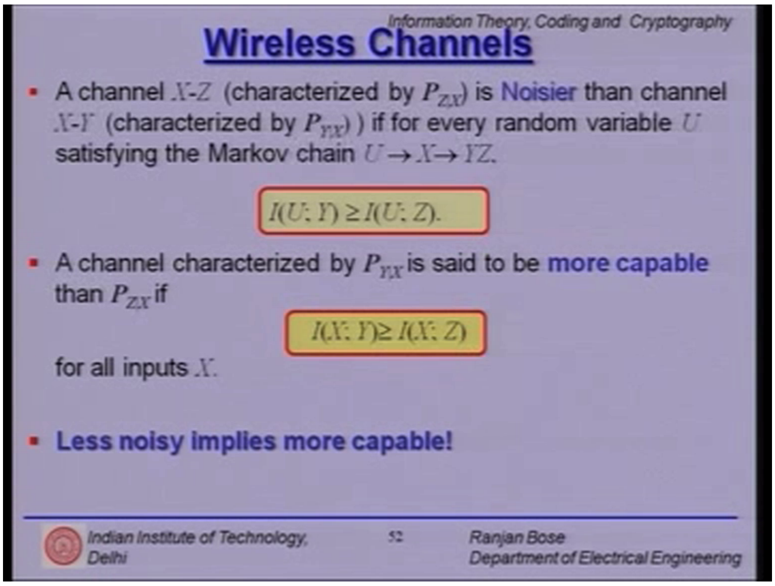
Observations

- Although, the DWTC is interesting mathematically, it is **not** a practical model for wireless communication scenarios.
- In wireless communications, the eavesdropper can simply 'stick-up' its antenna and 'listen in' without the trouble of 'tapping the wire'.
- Thus there will be a direct wireless channel to the legitimate receiver (main channel), and another wireless channel to the eavesdropper (eavesdropper channel).
- Another interesting thing about the wireless communication scenario is that **both** the legitimate receiver and the eavesdropper are free to move around.

Indian Institute of Technology, Delhi 51 Ranjan Bose Department of Electrical Engineering

So, this degraded wiretap channel model is interesting mathematically, but not practical for wireless scenarios, because in wireless scenario these eavesdropper can be present anywhere and it can stick up the antenna and listen in, so that both the legitimate receiver and eavesdropper are free to move around and the channels can be different better with respect to each other we have no control on that.

(Refer Slide Time: 36:33)



Information Theory, Coding and Cryptography

Wireless Channels

- A channel X-Z (characterized by P_{ZX}) is Noisier than channel X-Y (characterized by P_{YX})) if for every random variable U satisfying the Markov chain $U \rightarrow X \rightarrow YZ$.

$$\boxed{I(U; Y) \geq I(U; Z).}$$

- A channel characterized by P_{YX} is said to be more capable than P_{ZX} if

$$\boxed{I(X; Y) \geq I(X; Z)}$$

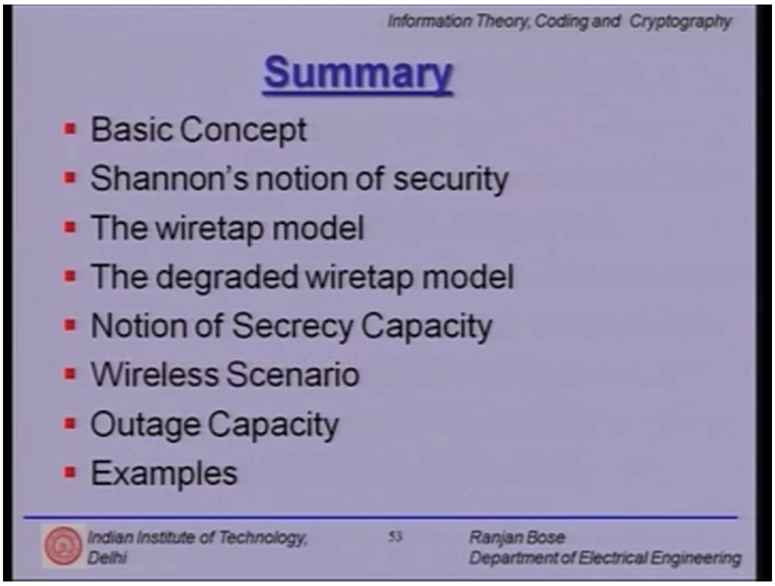
for all inputs X.

- **Less noisy implies more capable!**

Indian Institute of Technology, Delhi 52 Ranjan Bose Department of Electrical Engineering

So, a quick definition a channel X-Z characterized by the channel transition probability mat matrix P z given x is noisier than the channel X-Y characterized by P y given x if for every random variable U satisfying the Markov chain U arrow X arrow X Y Z. I have the mutual information I U semicolon Y greater than or equal to I U semicolon Z. A channel is characterized by P y given x and is said to be more capable than the channel P z given x if the mutual information I X semicolon Y is greater than or equal to I X semicolon Z for all inputs X. So, less noisy implies more capable.

(Refer Slide Time: 37:24)



Information Theory, Coding and Cryptography

Summary

- Basic Concept
- Shannon's notion of security
- The wiretap model
- The degraded wiretap model
- Notion of Secrecy Capacity
- Wireless Scenario
- Outage Capacity
- Examples

Indian Institute of Technology, Delhi 53 Ranjan Bose Department of Electrical Engineering

So, let us summarize what we have learn today. We started off with Shannon's notion of security. We talked about the wiretap model. We then moved on the degraded wiretap model. Subsequently, we introduce the notion of secrecy capacity. We talked about wireless scenario and we lead grounds for outage capacity, which we will talk about in the next class. We also looked at some examples along the way.

Thank you.