Simple and Efficient Single Round Almost Perfectly Secure Message Transmission Tolerating Generalized Adversary

Ashish Choudhury (ISI Kolkata, India)
Kaoru Kurosawa (Ibaraki Univ., Japan)
Arpita Patra (Aarhus Univ., Denmark)

Encryption Schemes

	Must share a secret-key	Don’t share a secret-key
Computational	SKE	PKE
Unconditional	One-time pad	

Does there exist ?

	Must share a secret-key	Don’t share a secret-key
Computational	SKE	PKE
Unconditional	One-time pad	???

Yes

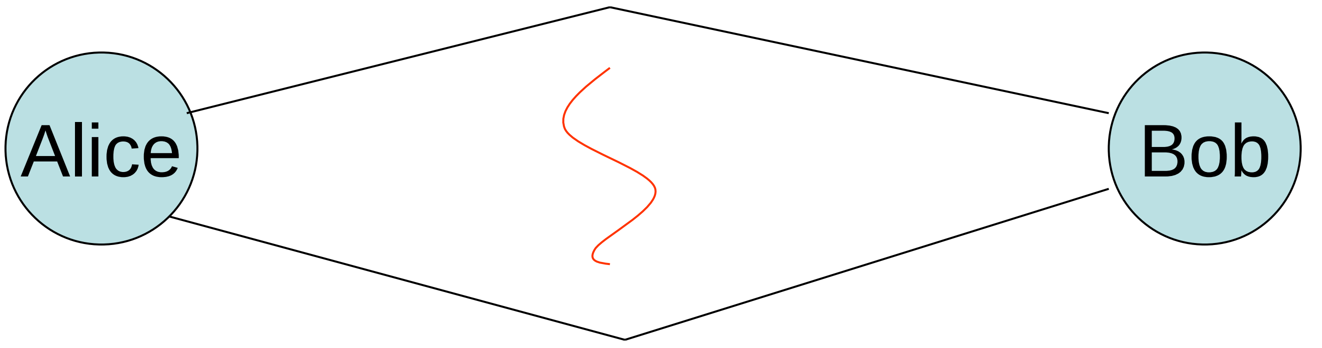
- (1975) Wyner

  Wire-tap channel model
- (1984) Bennett and Brassard

  BB84
- (1993) Dolev, Dwork, Waarts and Yung

  Network model

In the model of DDWY



- Alice and Bob are a part of a network
- There are n channels between them
- Adversary can corrupt (listen and forge)

    at most t channels

Indeed, in Internet

- There are many channels
  between A and B
- No adversary can corrupt all the routers

A scheme should satisfy

- (Perfect Privacy)

  Adversary learns no information on the secret message s
- (Perfect Reliability)

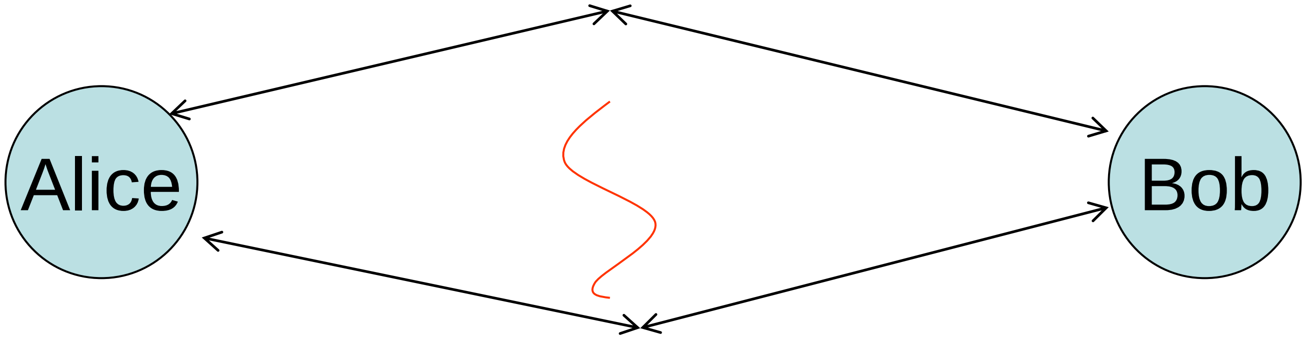
  Bob can receive s correctly

  (Adversary cannot forge s)

PSMT denotes

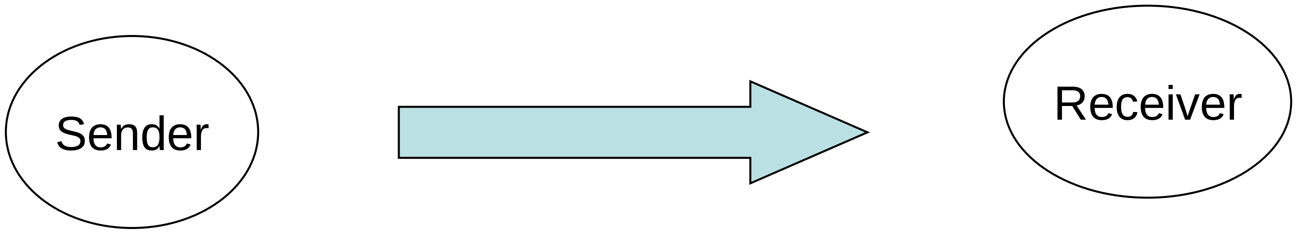
- Perfectly
- Secure
- Message
- Transmission
- Scheme

We consider an Undirected Network

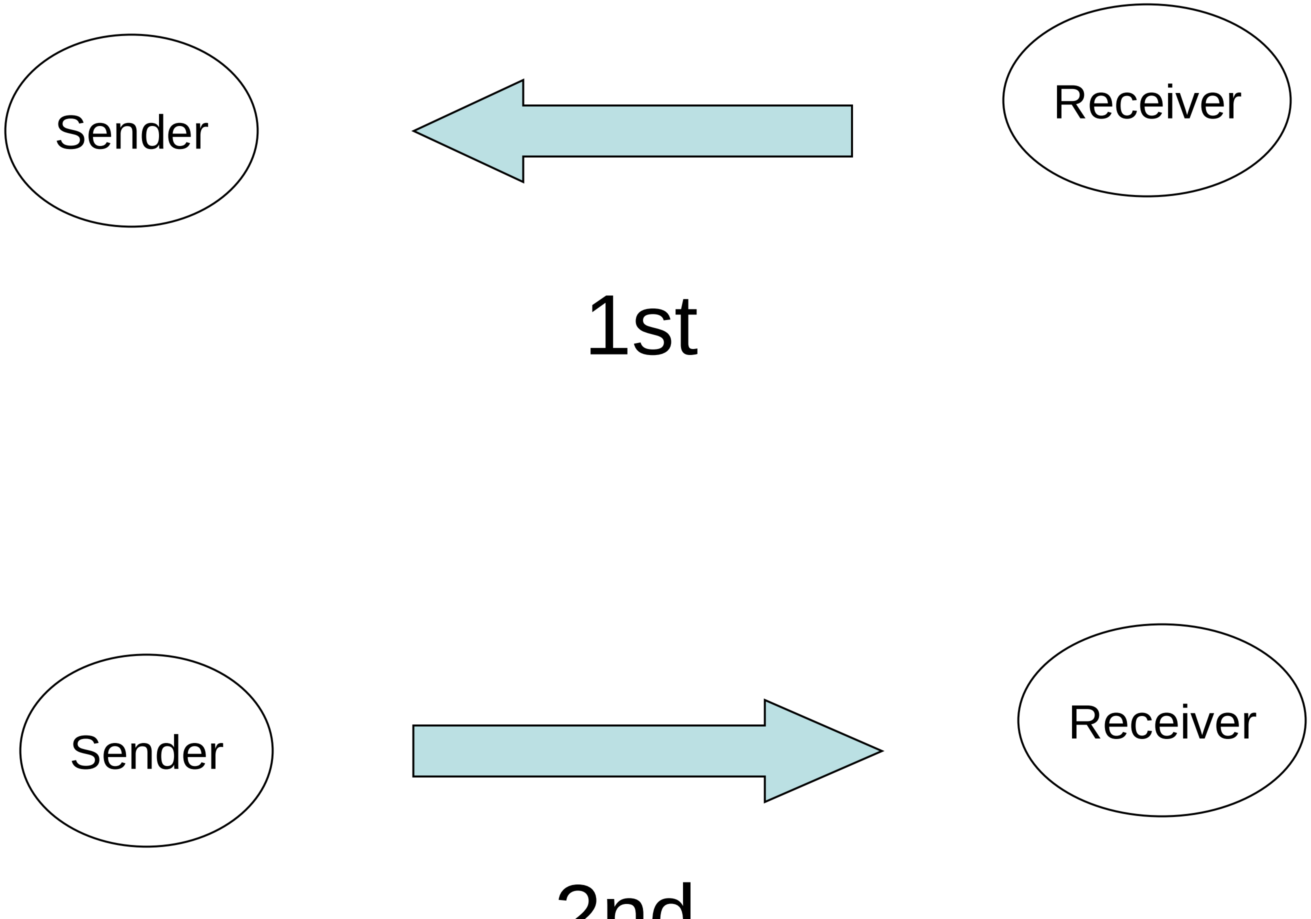


- Each channel is two-way

1 Round Protocol



2 Round Protocol



PSMT exists

1-round	iff $n \geqq 3t+1$
2-round	iff $n \geqq 2t+1$

where the adversary can corrupt
t out of n channels.

Almost PSMT

requires

- (Perfect Privacy)

  Adversary learns no information on the secret message s

- (Almost Perfect Reliability)

  Pr[Bob can receive s] > 1- ε

If $n \geqq 2t+1$,

PSMT requires	2 rounds
Almost PSMT requires	only 1 round

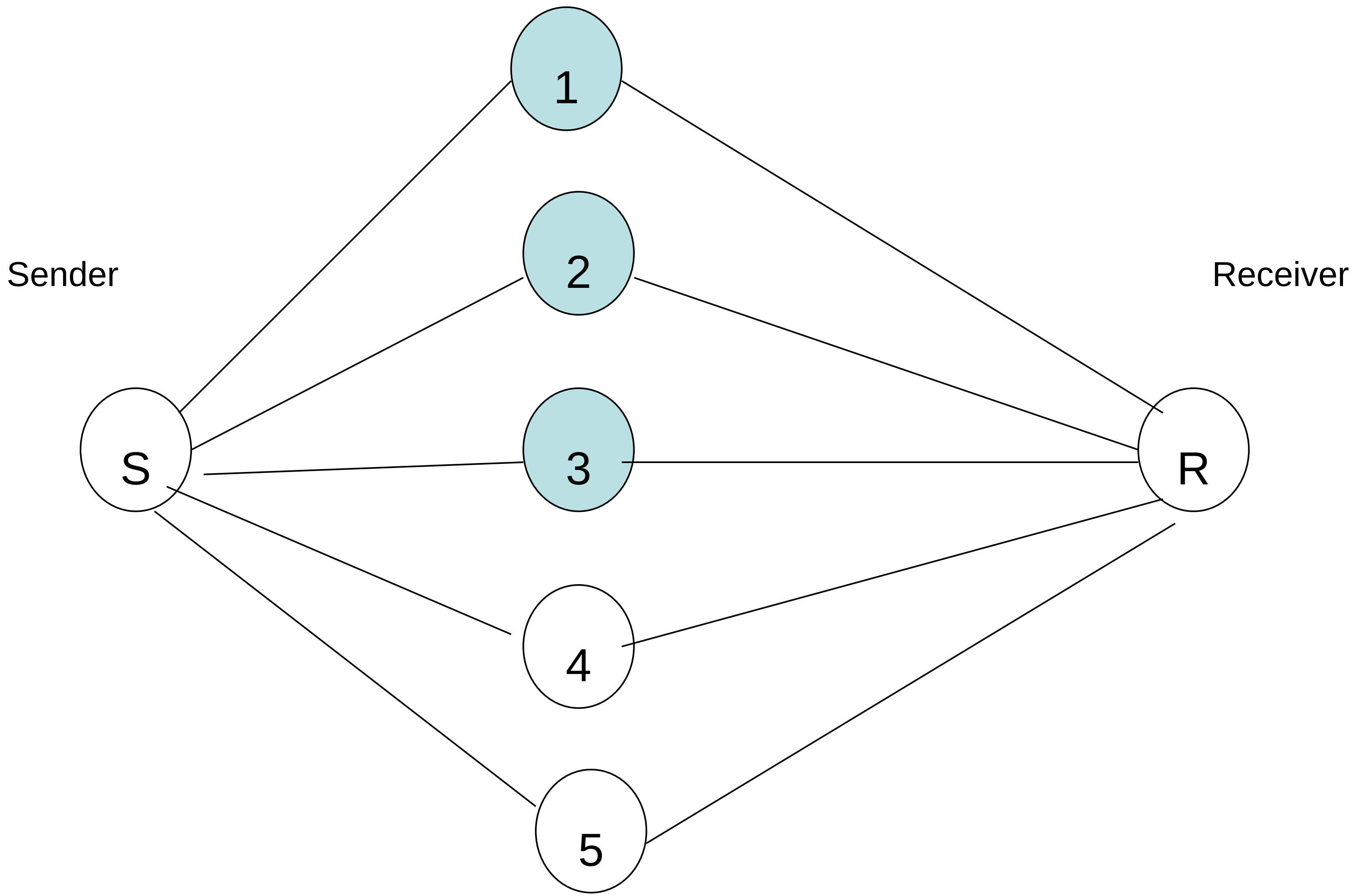
So far

	PSMT	**Almost PSMT**
Threshold adversary	We have seen	We have seen
How about General adversary	?	?

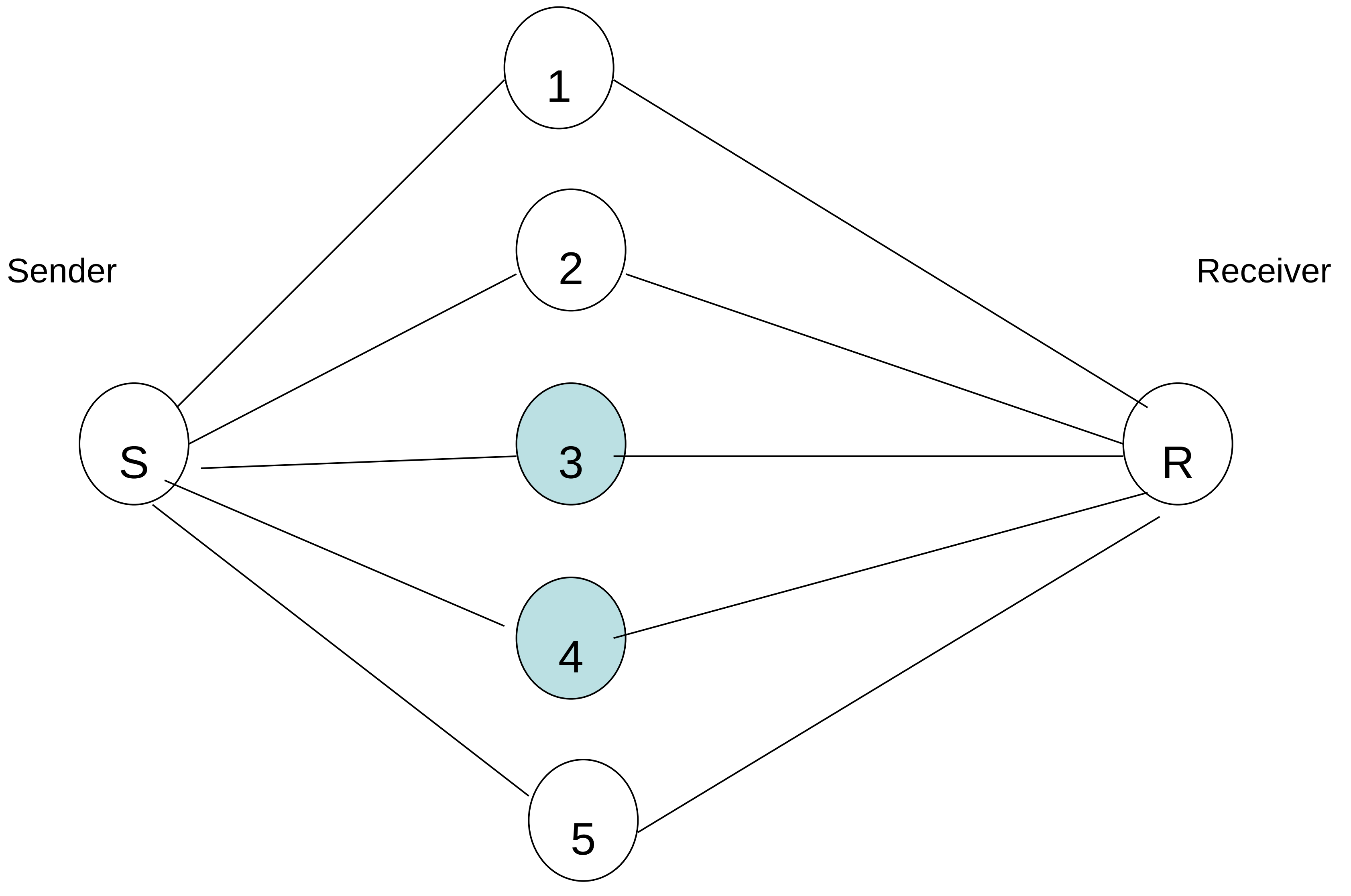
Desmedt et at.

- Threshold adversaries are not realistic
- when dealing with computer viruses,
- such as
- the I LOVE YOU virus
- and the Internet virus/worm
- that only spread to
- Windows, respectively Unix.

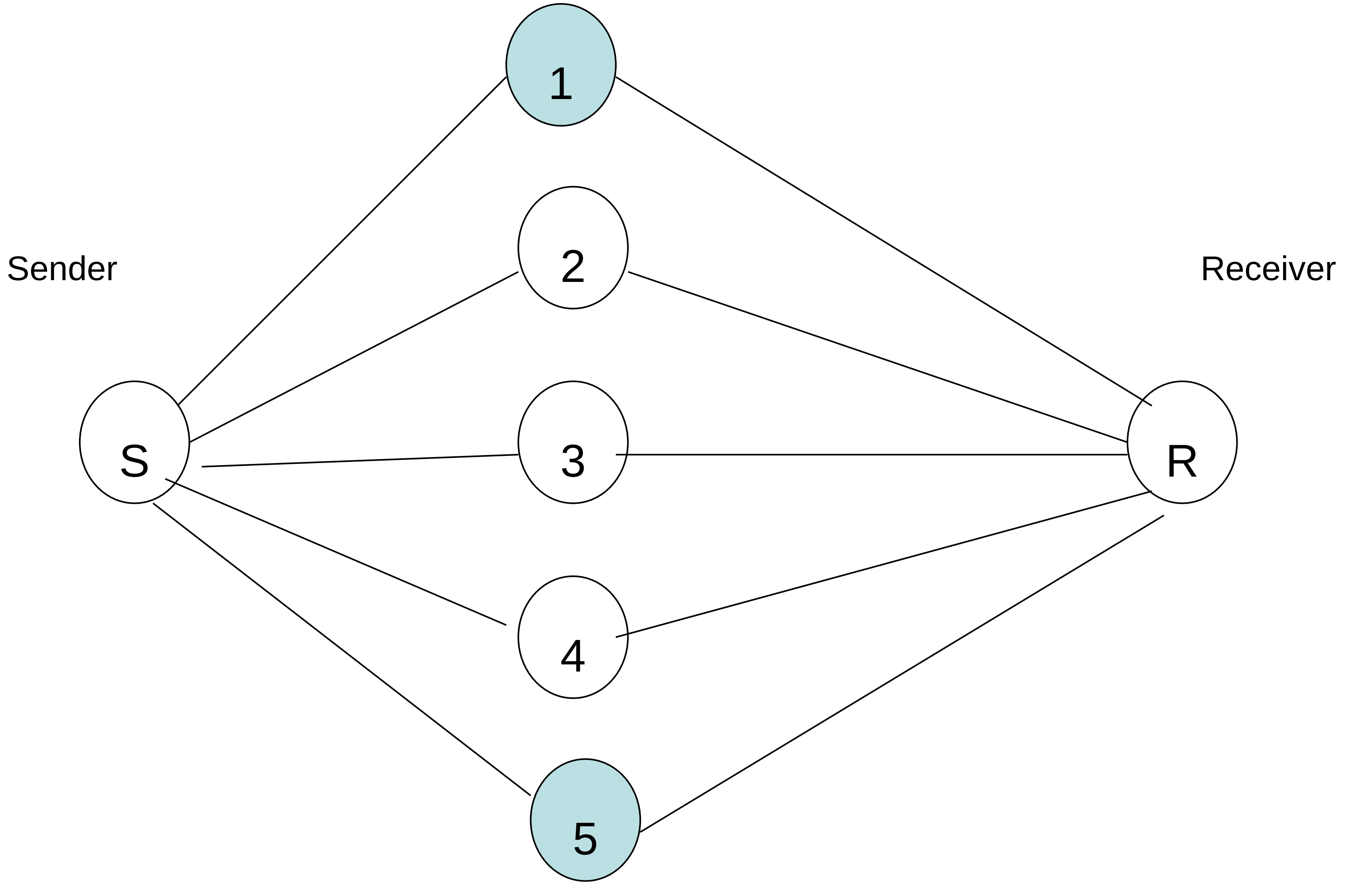
{1,2,3} use Windows



{3,4} use UNIX



{1,5} use TRON



Adversary can corrupt

$B_1=\{1,2,3\}$ or $B_2=\{3,4\}$ or $B_3=\{1,5\}$.

- Let

  $\Gamma=\{B_1, B_2, B_3\}$

- Such Γ is called an adversary structure.

Monotone

- We say that Γ is monotone
  if $B \in \Gamma$ and $B' \subset B$, then $B' \in \Gamma$
- For example.
  if an adversary can corrupt B={1,2,3},
  then she can corrupt B'={1,2} clearly.
- In what follows,
  we assume that Γ is monotone

Hirt and Maurer

- Introduced adversary structure
  in the context of multiparty protocols
- They generalized

  $n \geqq 2t+1$ to Q^2 adversary structure

  $n \geqq 3t+1$ to Q^3 adversary structure

Γ satisfies Q^2

- If

  $B_i \cup B_j \neq \{1, \cdots, n\}$

- for any $B_i, B_j \in \Gamma$

$\Gamma=\{B_1, B_2, B_3\}$

- Such that

  $B_1=\{1,2,3\}$, $B_2=\{3,4\}$, $B_3=\{1,5\}$.

- is Q^2 because

  $B_1 \cup B_2 = \{1,2,3,4\} \neq \{1, \cdots, 5\}$

  $B_1 \cup B_3 = \{1,2,3,5\} \neq \{1, \cdots, 5\}$

  $B_2 \cup B_3 = \{1,3,4,5\} \neq \{1, \cdots, 5\}$

Γ satisfies Q^3

- If

  $$B_i \cup B_j \cup B_k \neq \{1, \cdots, n\}$$

- for any $B_i, B_j, B_k \in \Gamma$

For general adversaries,

1-round PSMT	iff Γ satisfies Q^3
2-round PSMT	iff Γ satisfies Q^2

	PSMT	Almost PSMT
Threshold adversary	We have seen	We have seen
General adversary	We have seen	

? is

	PSMT	Almost PSMT
Threshold adversary	We have seen	We have seen
General adversary	We have seen	?

For the ?

- Patra, Choudhary, Srinathan, and Rangan
- showed an almost PSMT for Q^2.

However,

- At least 3 rounds
- Exponential time

This paper shows

- An efficient 1 round almost PSMT for Q^2

	# of rounds	Efficiency
Patra et al.	At least 3	Inefficient
Our scheme	1	Efficient

Hence
for Q^2 adversary structure,

PSMT requires	2 rounds
Almost PSMT requires	only 1 round (This paper)

In a Secret Sharing Scheme

- For a secret s,

  Dealer computes a share vector

  $$(\text{share}_1, \cdots , \text{share}_n),$$

  and gives share_i to player P_i

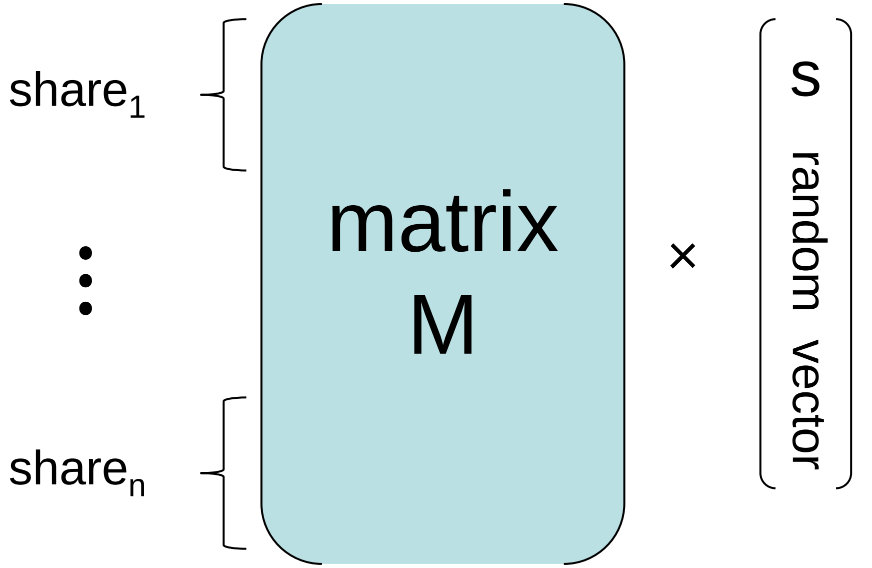
Proposition

For any adversary structure Γ,
there exists a linear secret sharing scheme (LSSS)
such that

- if $B \in \Gamma$, then B has no information on s
- if $A \notin \Gamma$, then A can reconstruct s

We call it an LSSS for Γ

In a LSSS



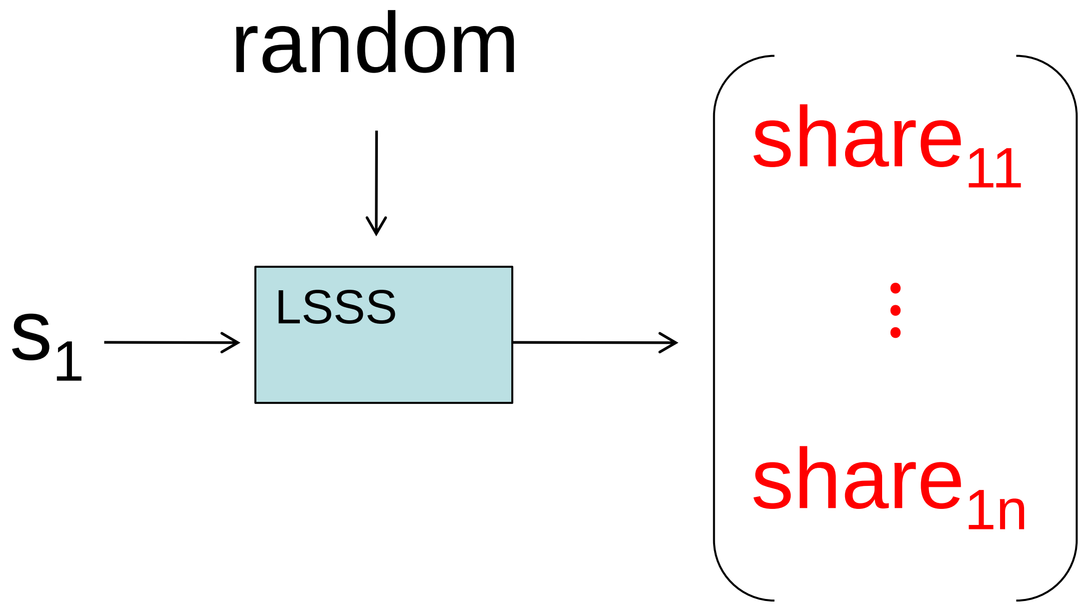
A share vector is computed by multiplying
(s, random vector)
to some matrix M

In our 1 round almost PSMT

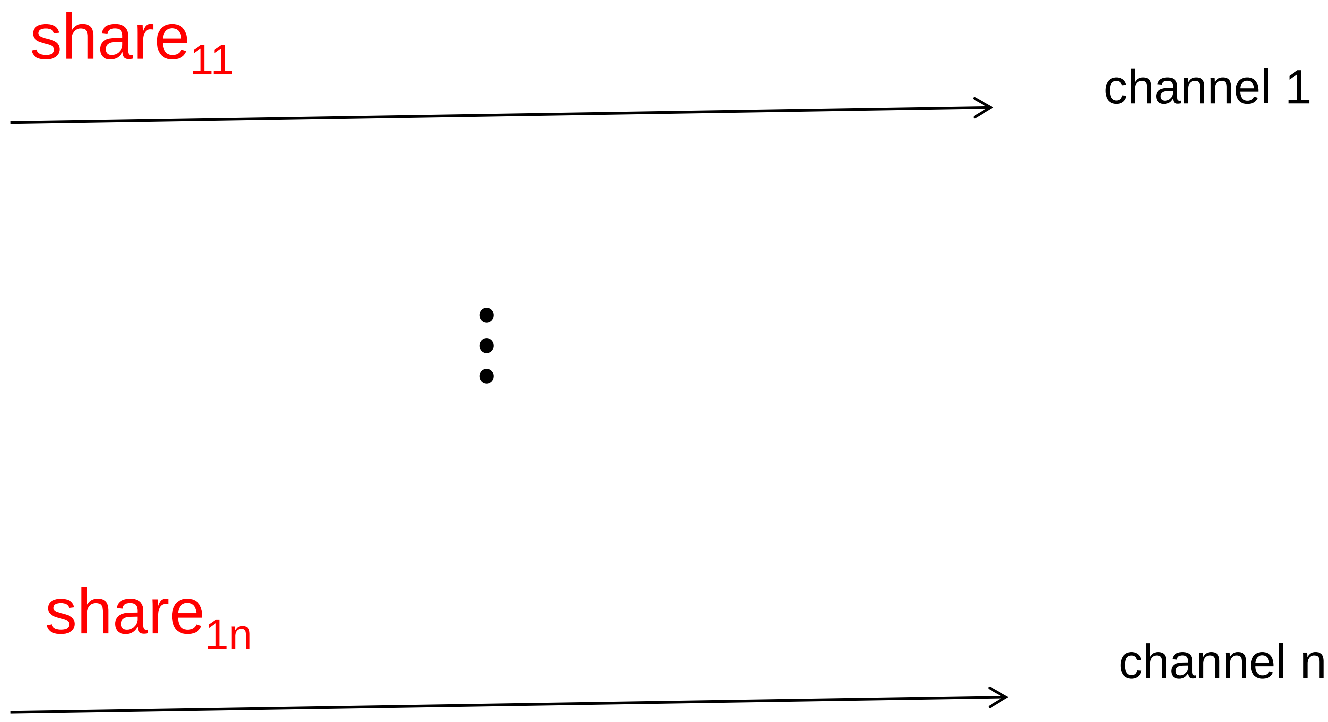
- We are given:
  - An adversary structure Γ satisfying Q^2 condition

- We then use an LSSS for this Γ
- Suppose that the sender wants to send a message $(s_1, \cdots, s_L)$ to the receiver.

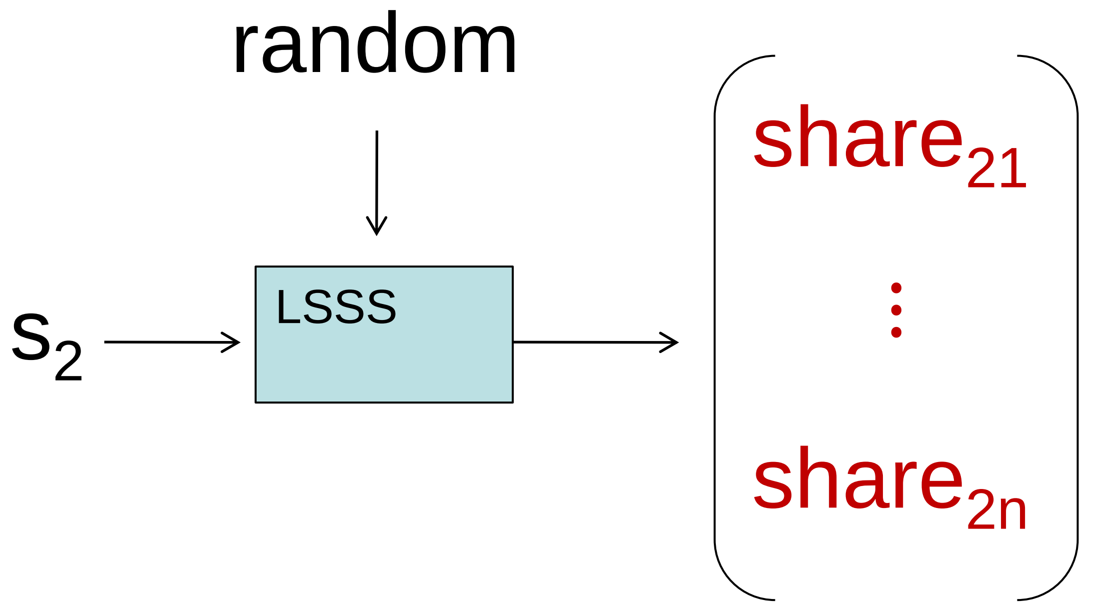
For s_1, sender computes



Sender sends to the receiver



For s_2, sender computes



Sender sends to the receiver

$share_{11}$, $share_{21}$ channel 1

⋮

$share_{1n}$, $share_{2n}$ channel n

and so on

$share_{11}$, $share_{21}$, ⋯, $share_{L1}$ → channel 1

⋮

$share_{1n}$, $share_{2n}$, ⋯, $share_{Ln}$ → channel n

Adversary learns no information on each s_i

- because Adv can listen to only a subset of channels $B \in \Gamma$
- From our property of the LSSS, $B \in \Gamma$ give no information on s_i

However

- Adv may forge the shares in B $\in \Gamma$
- To detect this forgery,

  Sender sends some additional authentication information.

To authenticate

$share_{11}, share_{21}, \cdots, share_{L1}$ → channel 1

⋮

$share_{1n}, share_{2n}, \cdots, share_{Ln}$ → channel n

We consider polynomials

$p_1(x) = share_{11} + share_{21}\, x + \cdots + share_{L1}\, x^{L-1}$

→ channel 1

⋮

$p_n(x) = share_{1n} + share_{2n}\, x + \cdots + share_{Ln}\, x^{L-1}$

→ channel n

To authenticate $p_1(x)$

$p_1(x) = share_{11} + share_{21}\, x + \cdots + share_{L1}\, x^{L-1}$

channel 1

random α_2 and $p_1(\alpha_2)$

channel 2

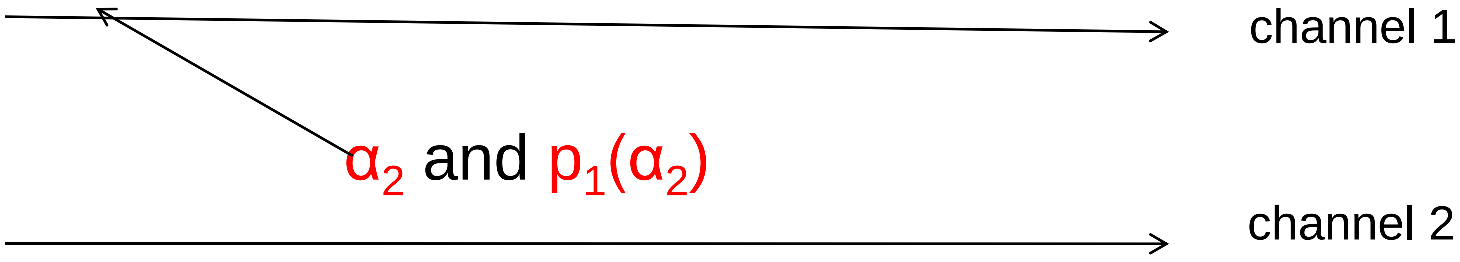
⋮

random α_n and $p_1(\alpha_n)$

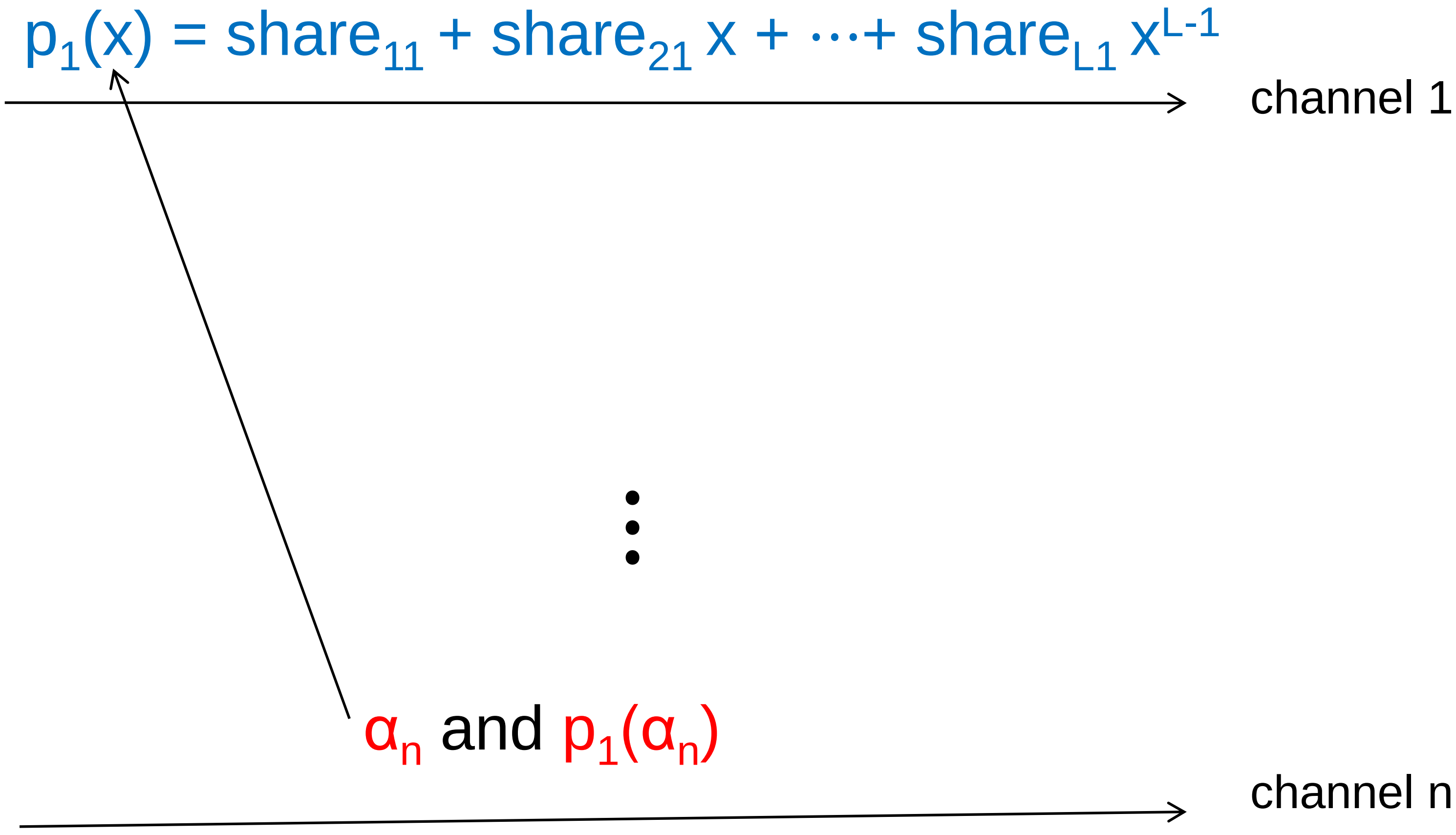
channel n

Receiver substitutes $x=\alpha_2$

$p_1(x) = share_{11} + share_{21}\, x + \cdots + share_{L1}\, x^{L-1}$



R substitutes $x=\alpha_n$



Suppose that $p_1(x)$ is forged

$$p_1(x) = share_{11} + share_{21}\, x + \cdots + share_{L1}\, x^{L-1}$$

channel 1 is corrupted

α_2 and $p_1(\alpha_2)$

channel 2 is not corrupted

$$Pr_{\alpha 2}\,[\, p_1(\alpha_2) = p_1(\alpha_2)\,] \leqq (L-1)/|F|$$

where $L-1=\deg p_1(x)$ and
the LSSS is computed over a finite field F

But

- Suppose that channel 1 is not corrupted and channel i is corrupted.
- Then

  $(\alpha_i, p_1(\alpha_i))$ leaks some information on

  $p_1(x) = share_{11} + share_{21}\, x + \cdots + share_{L1}\, x^{L-1}$

Sender hides $p_1(\alpha_i)$ as follows

$p_1(x)$ and $k_{12}, \cdots, k_{1n}$ → channel 1

α_2 and $p_1(\alpha_2)+k_{12}$ → channel 2

⋮

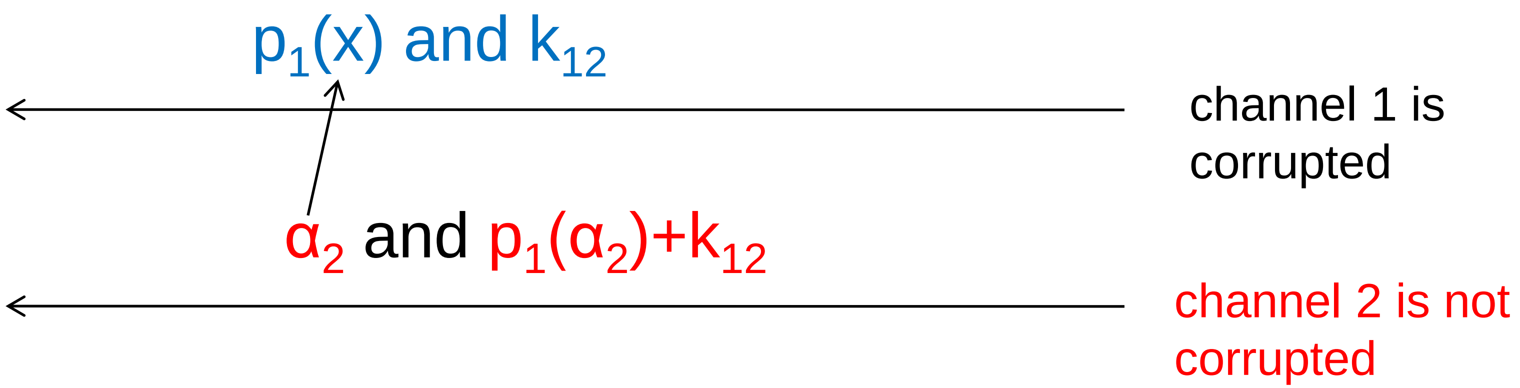
α_n and $p_1(\alpha_n)+k_{1n}$ → channel n

This is one-time pad

We do the same thing

- For $p_2(x)$, …, $p_n(x)$

Again forged $p_1(x)$ is detected



with

$$\Pr_{\alpha 2}\left[\, p_1(\alpha_2) + k_{12} \neq p_1(\alpha_2) + k_{12} \,\right] \geqq 1 - (L-1)/|F|$$

Lemma

- If $p_1(x)$ is forged,
- then

it is rejected by a correct channel i

with prob.

$$1-\frac{L-1}{|F|}$$

Next Receiver

- Reconstructs the message

  $(s_1, \ldots, s_L)$

  as follows.

Proposition

- If Γ is Q^2, then for any $B \in \Gamma$,

  $B^c \notin \Gamma$

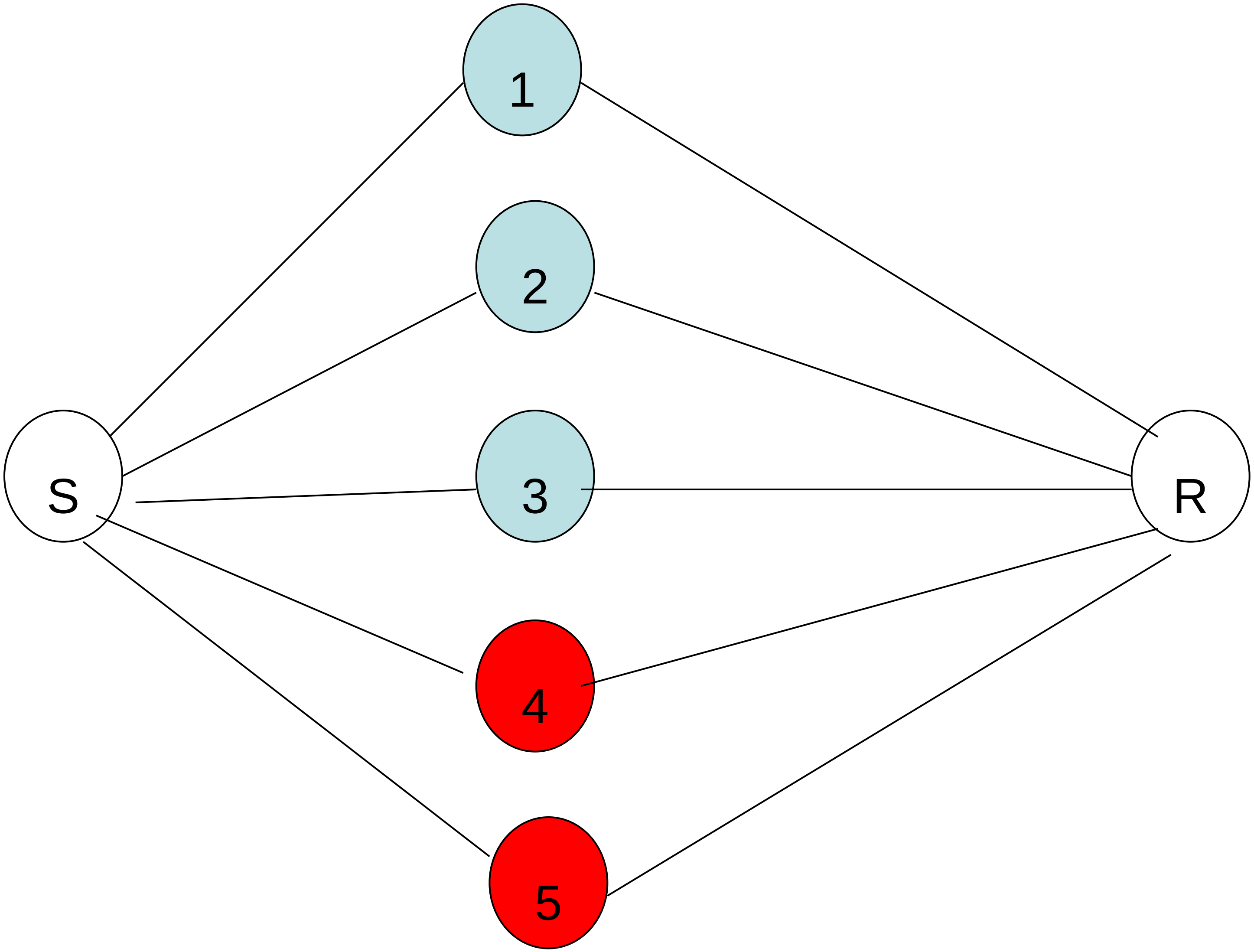
(Proof)

- Suppose that $B^c \in \Gamma$.
- Then

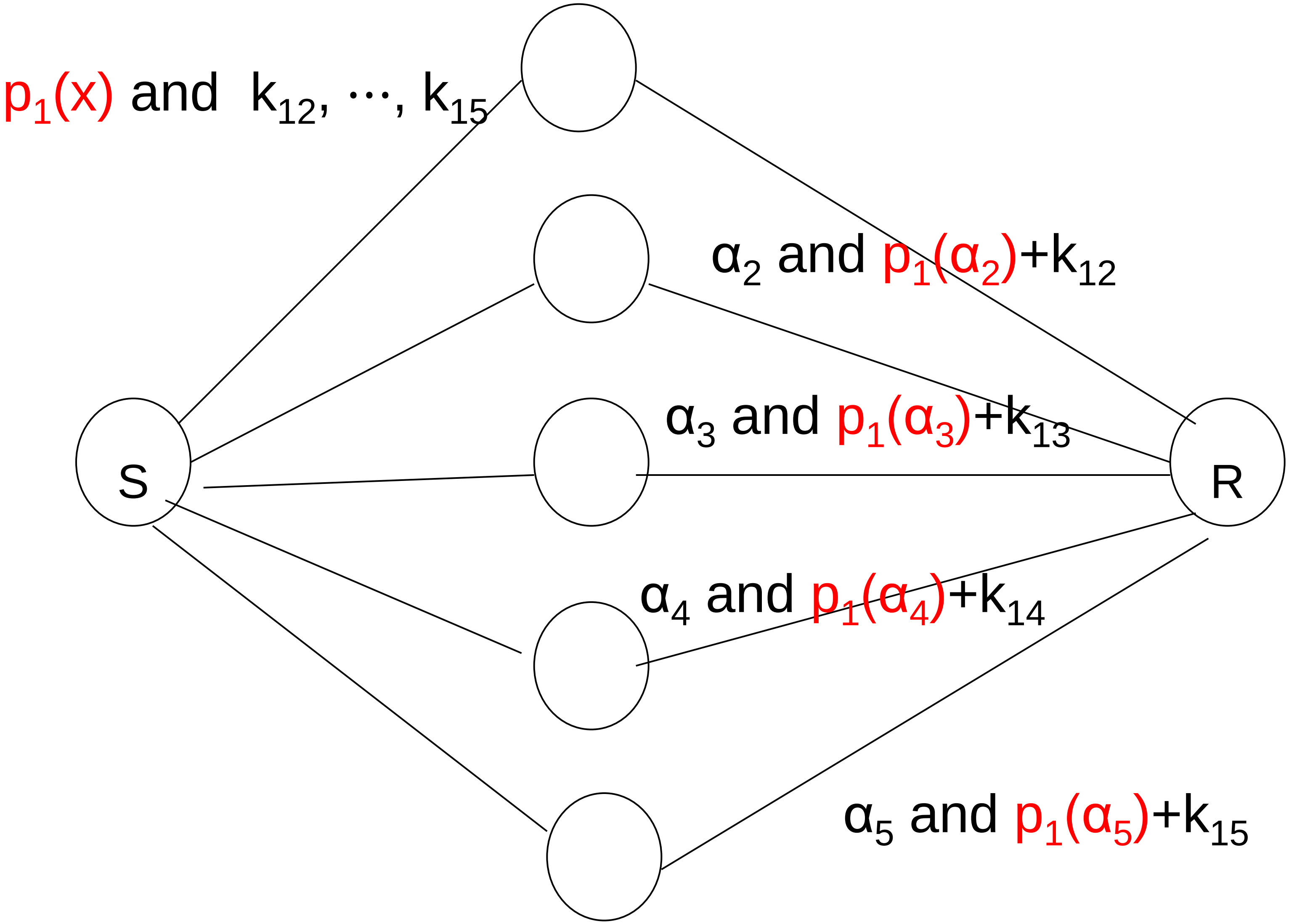
  B and $B^c \in \Gamma$

  $B \cup B^c = \{1, \cdots, n\}$
- This is against Q^2

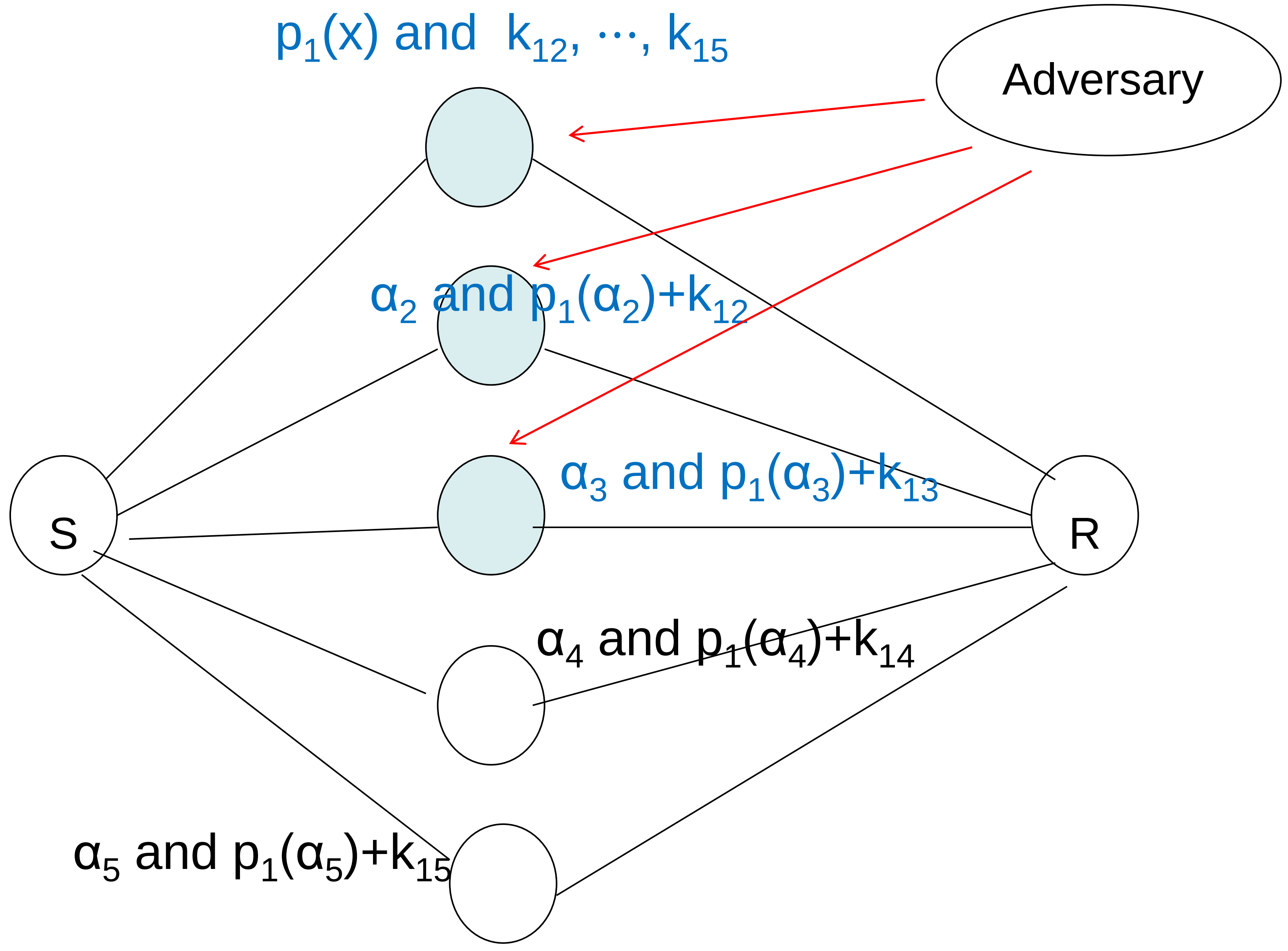
$$\{1,2,3\} \in \Gamma \text{ and } \{4,5\} \notin \Gamma$$

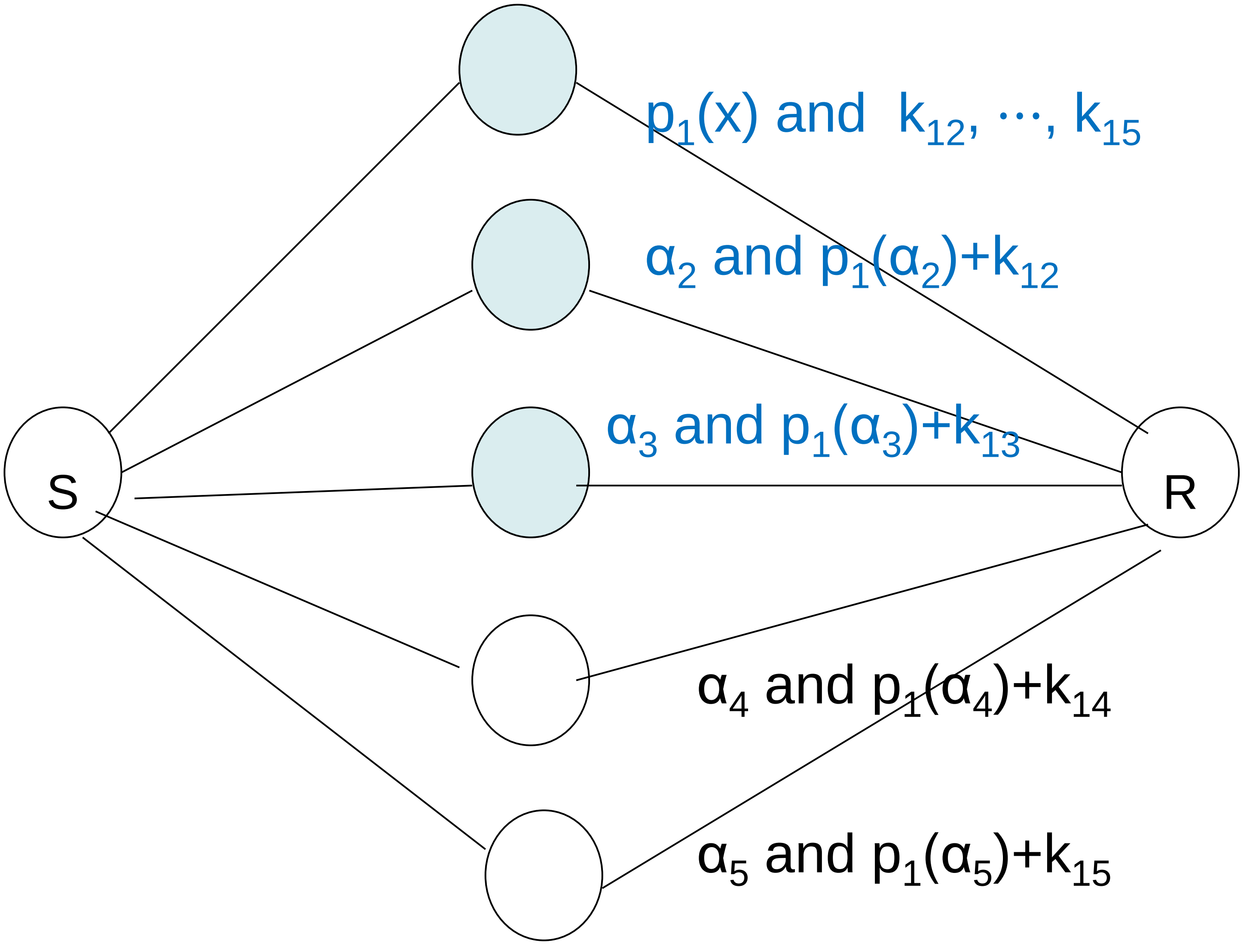


Look at $p_1(x)$

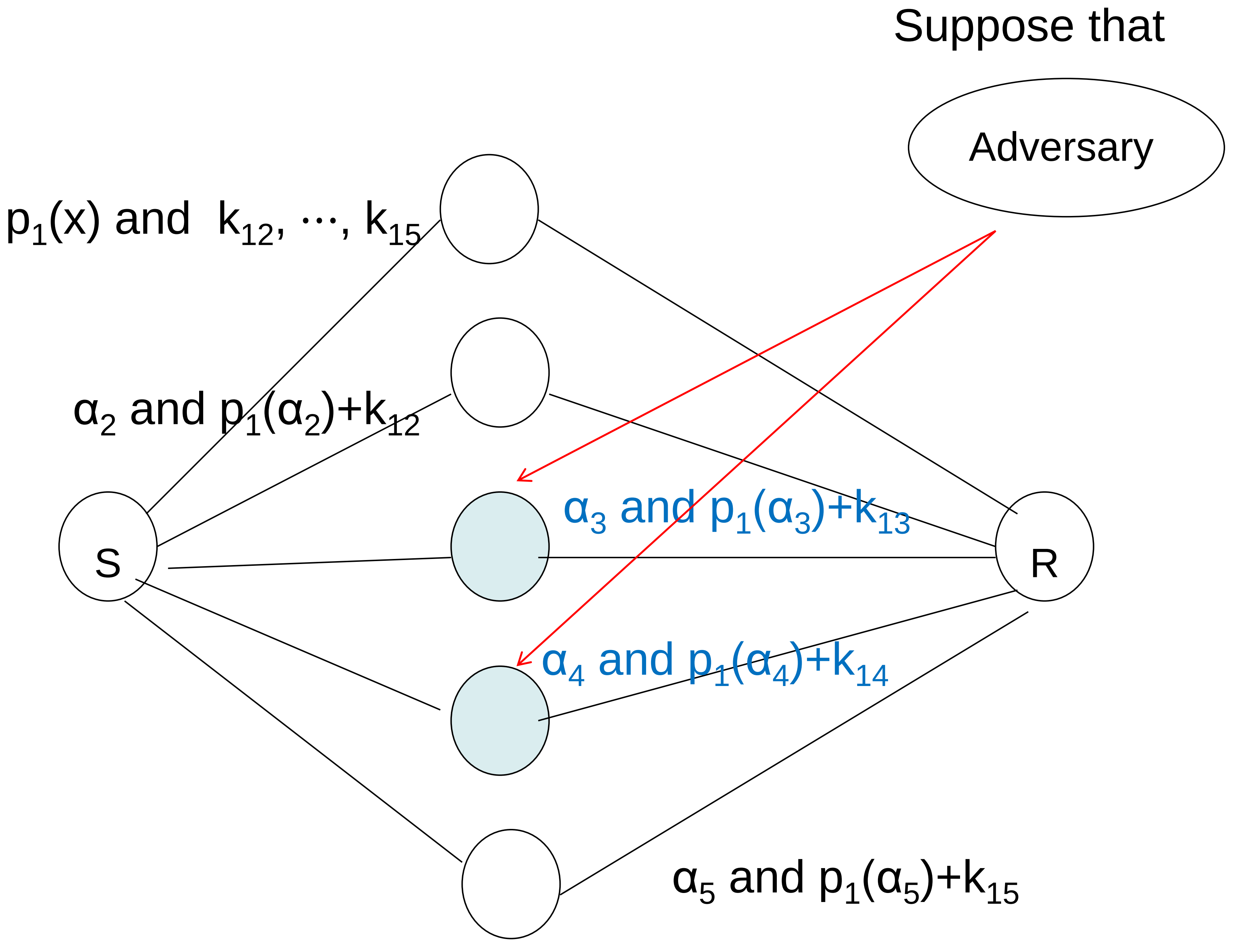

$p_1(x)$ and $k_{12}, \cdots, k_{15}$
α_2 and $p_1(\alpha_2)+k_{12}$
α_3 and $p_1(\alpha_3)+k_{13}$
S
R
α_4 and $p_1(\alpha_4)+k_{14}$
α_5 and $p_1(\alpha_5)+k_{15}$

Suppose that



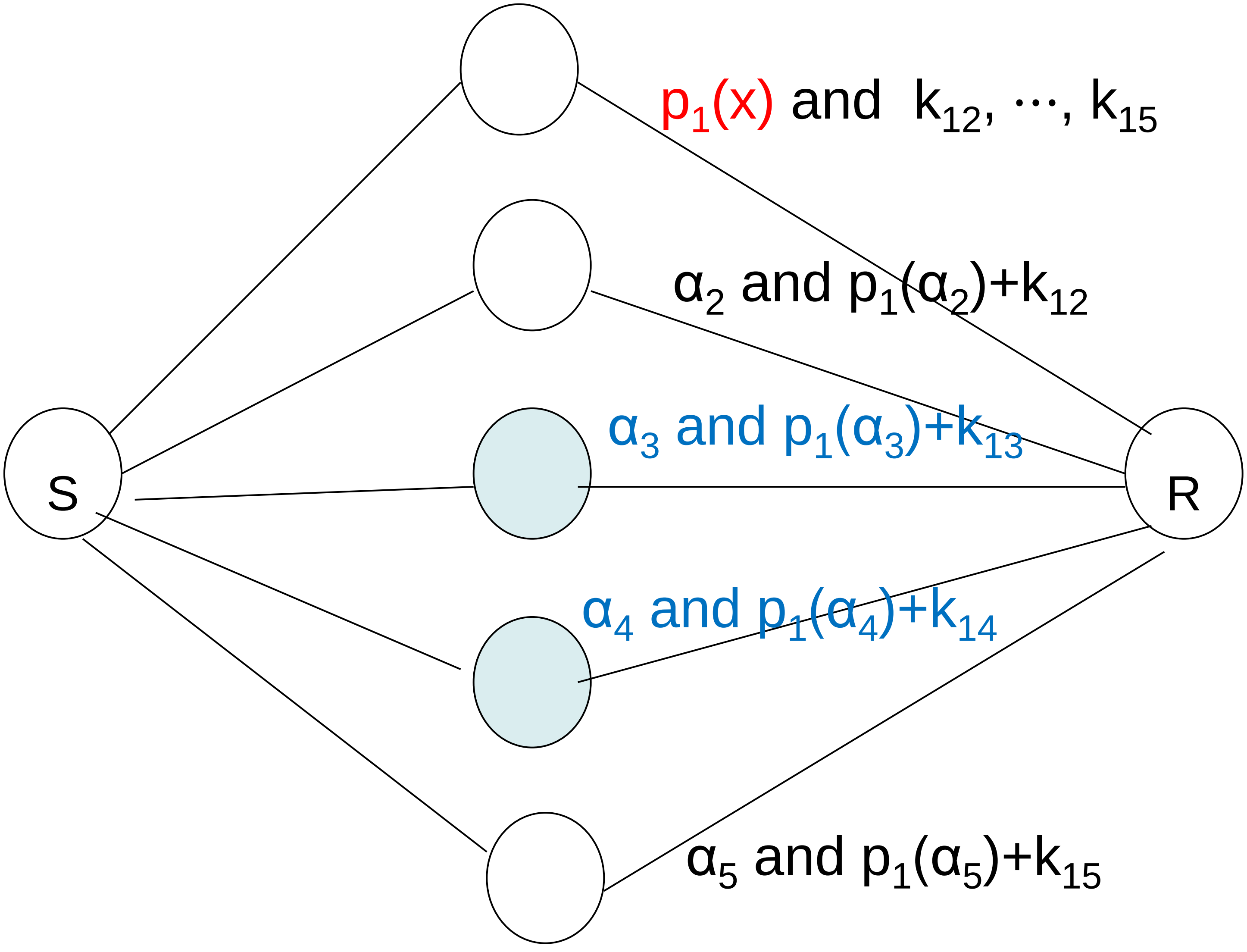


Then the forged $p_1(x)$ is rejected by channels {4 and 5} $\notin \Gamma$



Suppose that
Adversary
p1(x) and k12, ⋯, k15
α2 and p1(α2)+k12
α3 and p1(α3)+k13
S
R
α4 and p1(α4)+k14
α5 and p1(α5)+k15

In this case, $p_1(x)$ is not forged and
$p_1(x)$ is rejected by channels {3 and 4} ∈ Γ



Hence

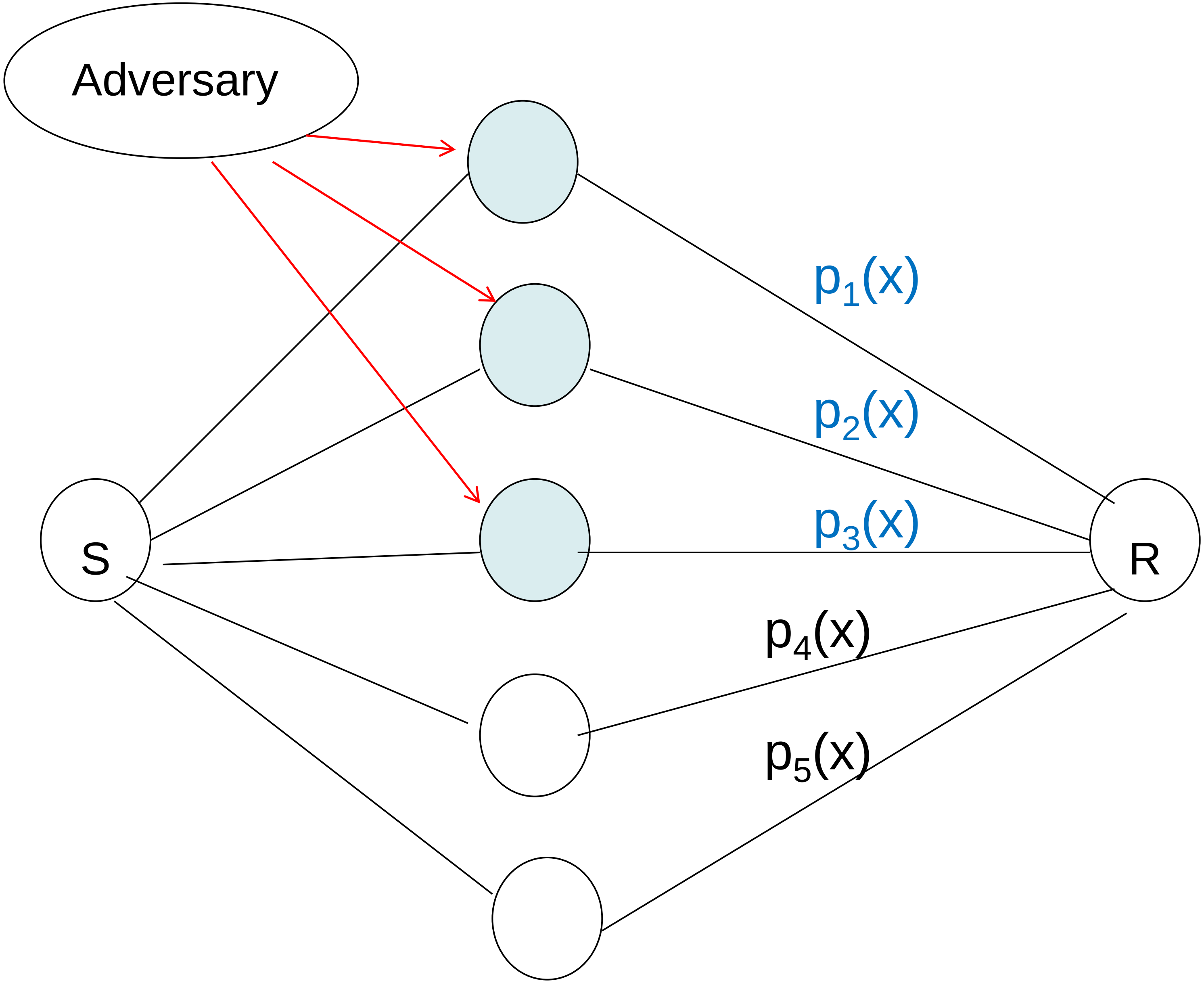
	then $p_1(x)$ is rejected
If $p_1(x)$ is forged,	by some $A \notin \Gamma$
If $p_1(x)$ is not forged,	by some $B \in \Gamma$

So Receiver behaves as follows

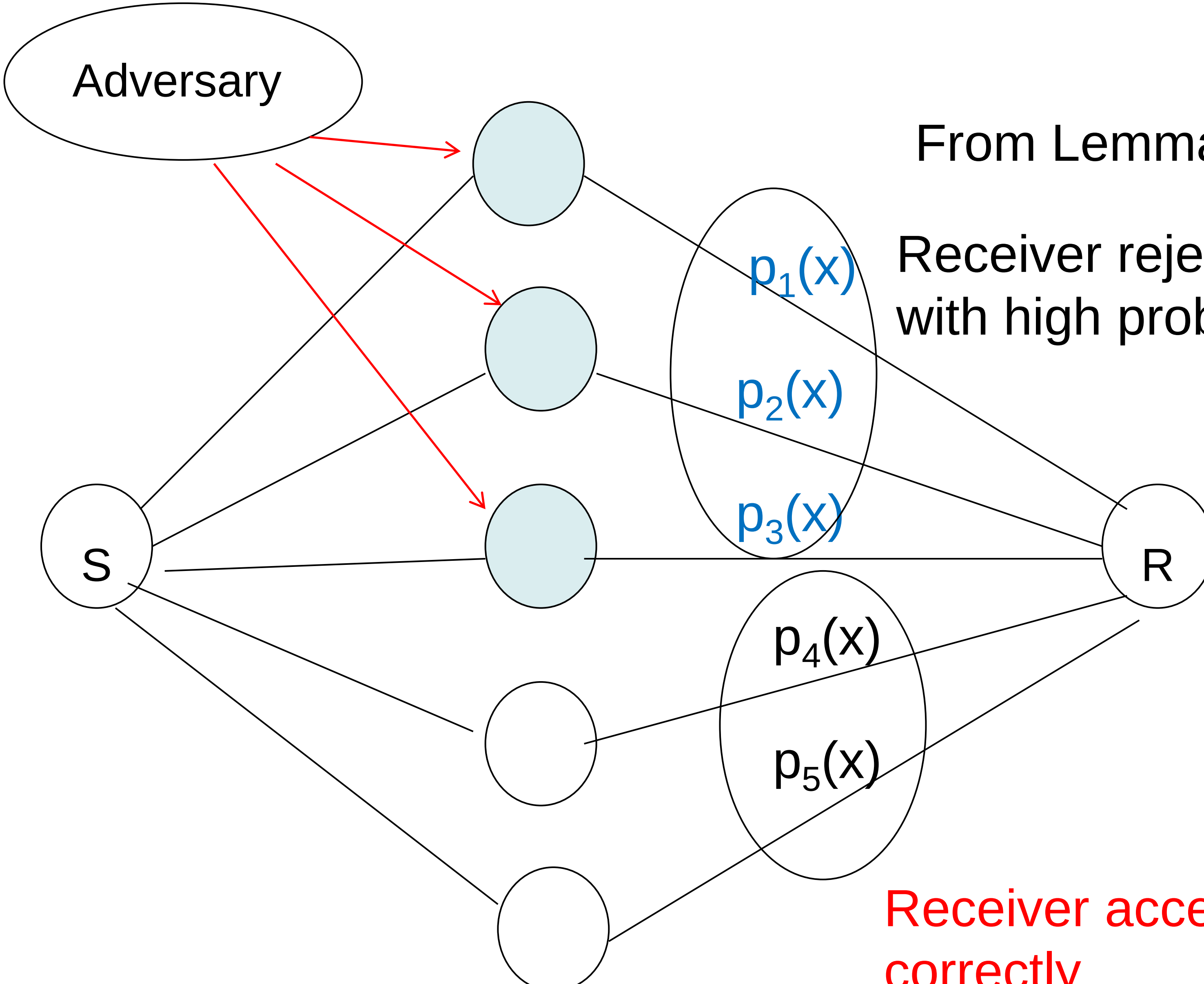
If $p_1(x)$ is rejected	Then Receiver
by some $A \notin \Gamma$	rejects $p_1(x)$
by some $B \in \Gamma$	accepts $p_1(x)$

Lemma

- If $p_1(x)$ is forged,
  R rejects it with high probability
- Otherwise
  R accepts it correctly



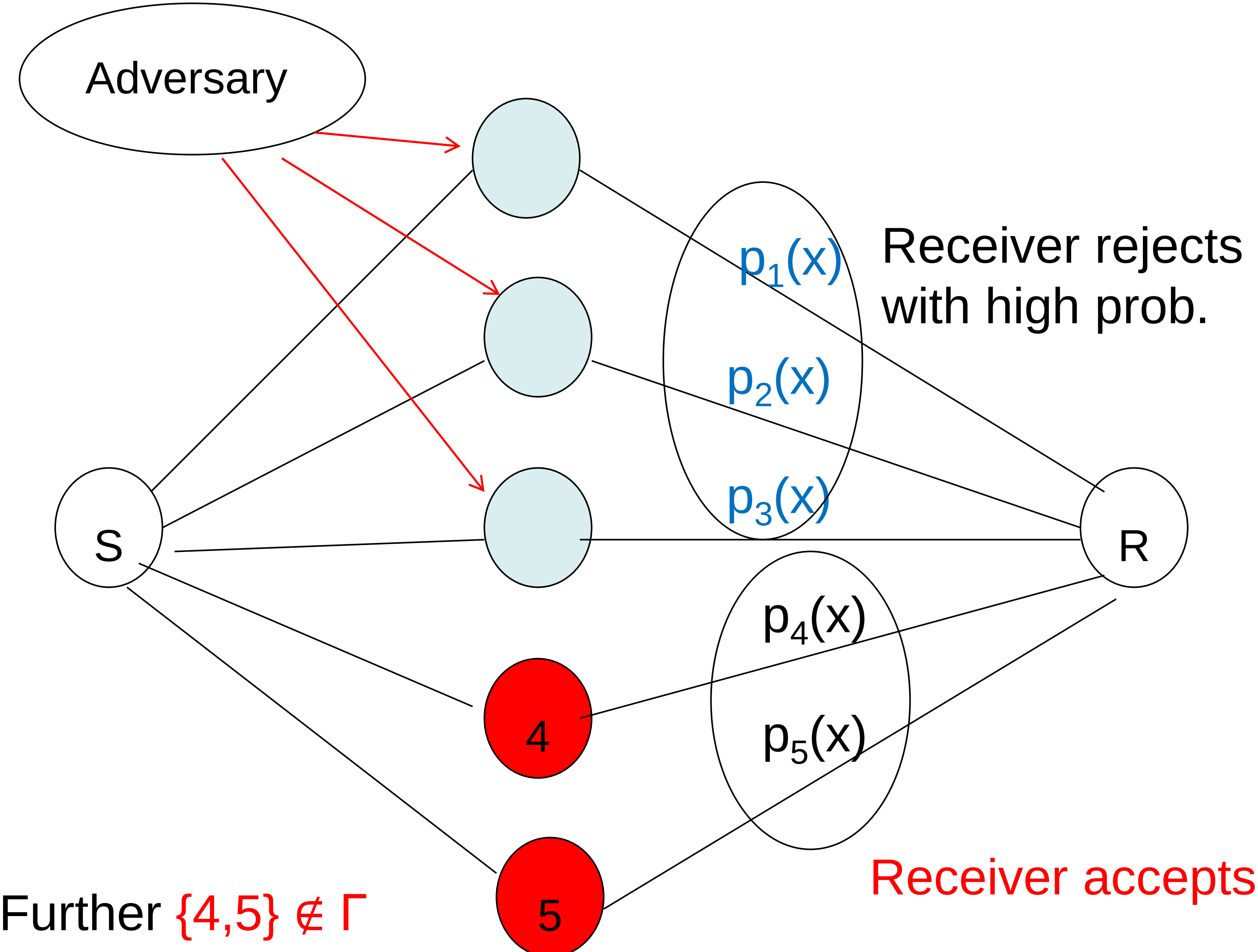
Adversary
S
R
$p_1(x)$
$p_2(x)$
$p_3(x)$
$p_4(x)$
$p_5(x)$



From Lemma,

Receiver rejects with high prob.

Receiver accepts correctly



Further {4,5} $\notin \Gamma$

Hence

{4,5} is an access set of the LSSS

Receiver accepts

$$p_4(x) = share_{14} + share_{24}\, x + \cdots + share_{L4}\, x^{L-1}$$

$$p_5(x) = share_{15} + share_{25}\, x + \cdots + share_{L5}\, x^{L-1}$$

Since {4,5} is an access set of the LSSS

$p_4(x) = share_{14} + share_{24}\, x + \cdots + share_{L4}\, x^{L-1}$

$p_5(x) = share_{15} + share_{25}\, x + \cdots + share_{L5}\, x^{L-1}$

$\downarrow$

s_1

Receiver can reconstruct

Since {4,5} is an access set

$p_4(x) = share_{14} + share_{24} x + \cdots + share_{L4} x^{L-1}$

$p_5(x) = share_{15} + share_{25} x + \cdots + share_{L5} x^{L-1}$

$\downarrow$ s_1 $\downarrow$ s_2

Receiver can reconstruct

Since {4,5} is an access set

$$p_4(x) = share_{14} + share_{24}x + \cdots + share_{L4}\, x^{L-1}$$

$$p_5(x) = share_{15} + share_{25}\, x + \cdots + share_{L5}\, x^{L-1}$$

$\downarrow$ $\qquad$ $\downarrow$ $\qquad$ $\downarrow$

s_1 $\qquad$ s_2 $\qquad$ $\cdots$ $\qquad$ s_L

Receiver can reconstruct

Theorem

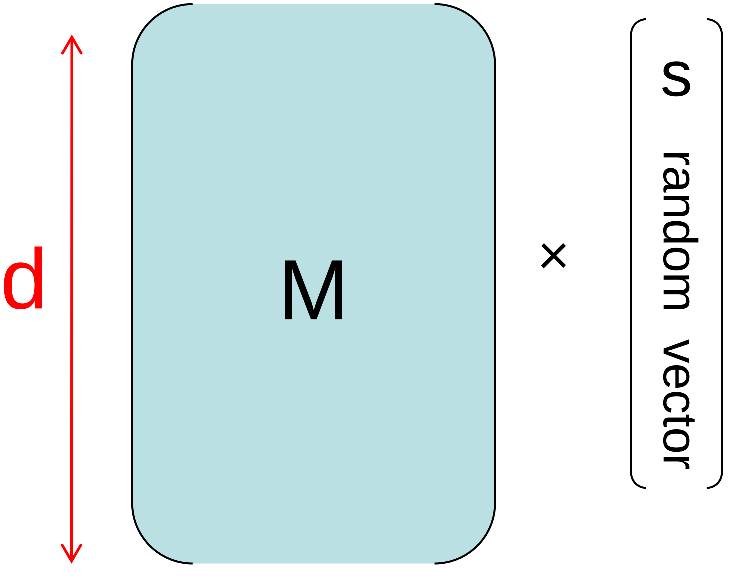
- Our protocol satisfies perfect privacy
- It also satisfies almost perfect reliability

The computational cost

- is polynomial in the size of the LSSS

The size of LSSS (=d)

is the # of rows of the matrix M



The communication cost

- Sender sends $O(Ld+d^2)$ field elements, where d is the size of the LSSS

As a special case,

- For threshold adversaries s.t. n≧2t+1, (adversary can corrupt t channels),
- our scheme is more efficient and simpler than the existing almost PSMT

Lower bound

- For threshold adversaries given by Patra, Choudhary, Srinathan and Rangan

- In any 1-round almost PSMT with $n=2t+1$, Sender must send $\Omega(nL)$ field elements to send a message $(s_1, \cdots, s_L)$

Patra et al. also showed

- A construction of
  1-round almost PSMT for n=2t+1
  which satisfies their bound

However

- It is complex
- It uses extrapolation technique, extracting randomness and etc.

Our almost PSMT

- Also satisfies the bound of Patra et al.
  if L $\geqq$ n
- Further
  it is more efficient and much simpler

Summary

We showed an efficient
1-round almost PSMT for Q^2

PSMT requires	2 rounds
Almost PSMT requires	only 1 round (This paper)

As a special case,

- For threshold adversaries s.t. $n \geqq 2t+1$,
- our scheme is more efficient and simpler than the previous almost PSMT