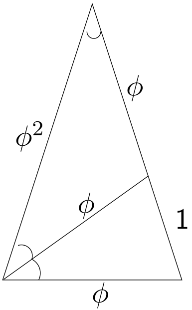
# Investigating the Fundamental Communication Burden of Distributed Cooperation

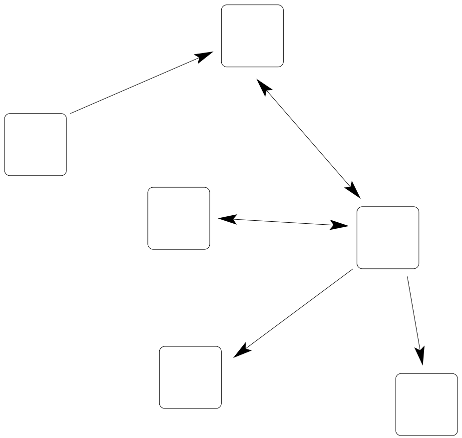
Paul Cuff
(with Tom Cover and Haim Permuter)

Stanford University

February 11, 2009



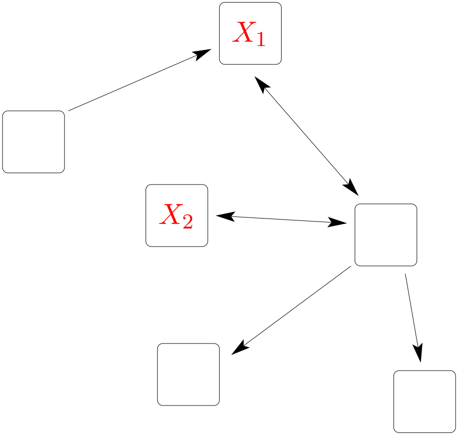
# Overview



Other work moving information in networks:

- The Gossiping Dons Problem [Bollobas, The Art of Mathematics]
- Distributed Average Consensus

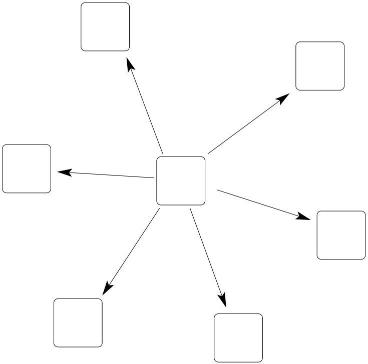
# Overview




Other work moving information in networks:

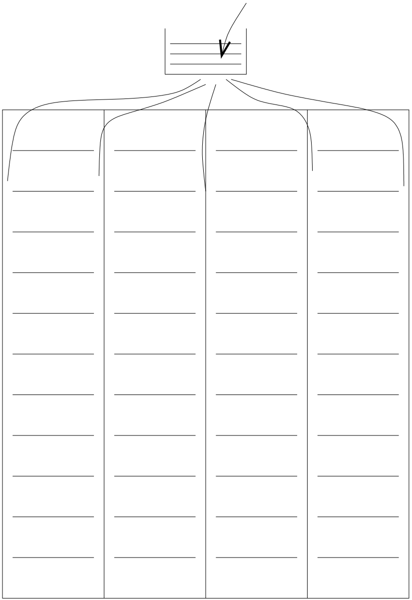
- The Gossiping Dons Problem [Bollobas, The Art of Mathematics]
- Distributed Average Consensus

# Talk Assignment in Networks



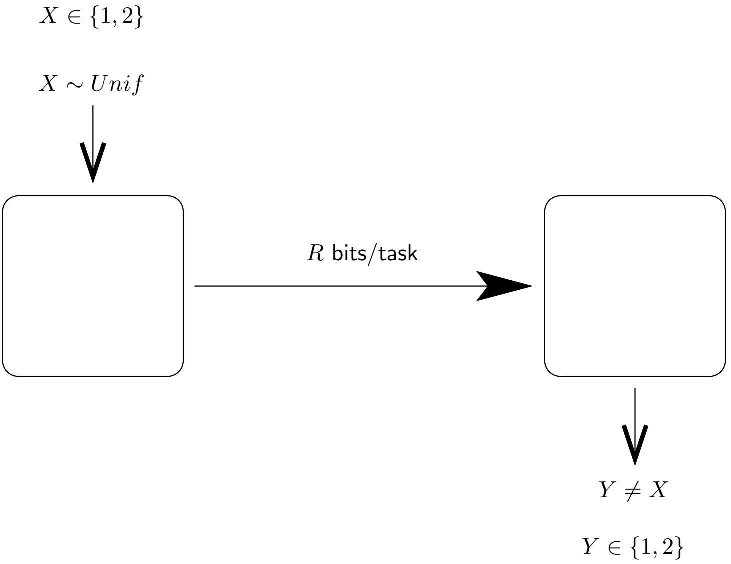
Computation tasks numbered $1, ..., k$ must be assigned uniquely.

# Data Center



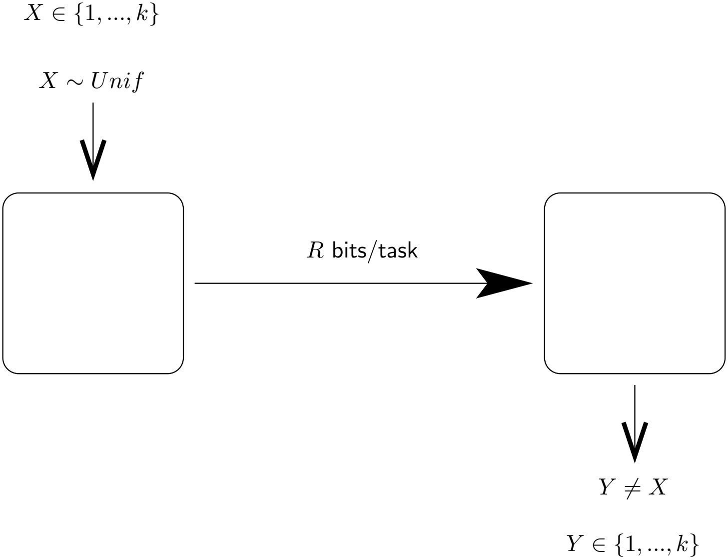
# Two Nodes

Tasks are assigned to numbers.



# Two Nodes

Tasks are assigned to numbers.



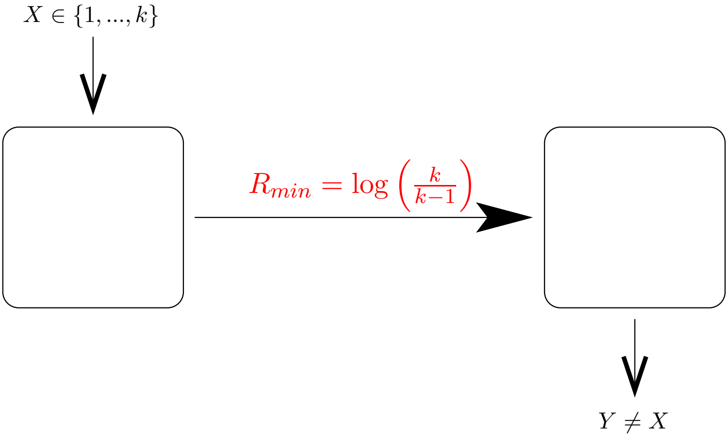
# Rate-Distortion Result

$$R_{min} = \min_{p(y|x)} I(X;Y)$$

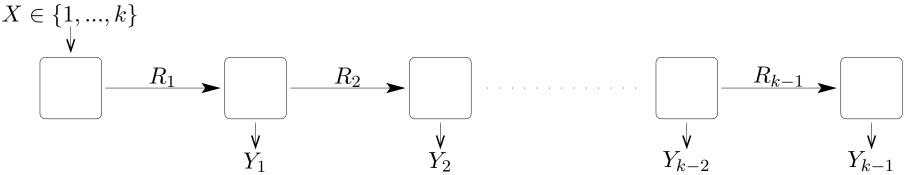
such that $X \neq Y$ with probability 1.

# Two Node Result

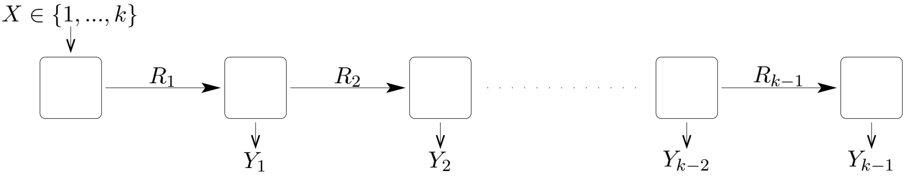
Optimal two node task assignment rate:



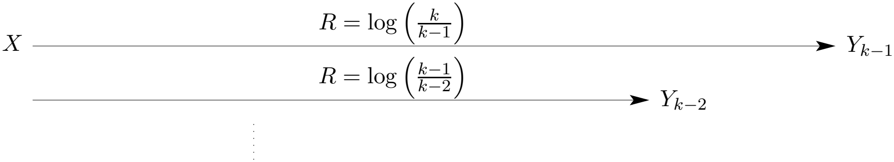
# Cascade - One Assigned



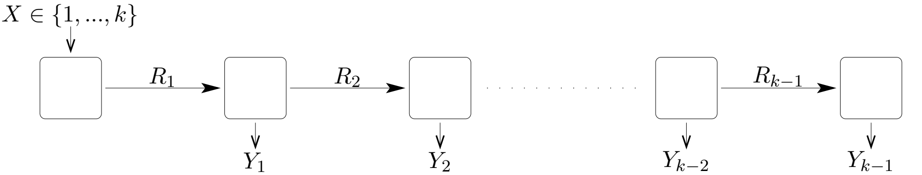
# Cascade - One Assigned



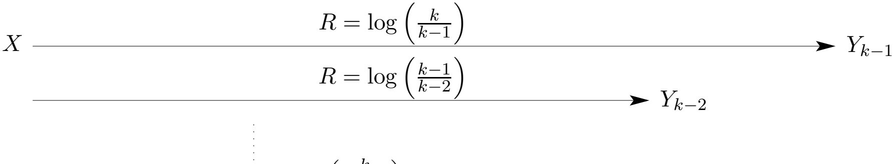

Optimal Communication:



# Cascade - One Assigned

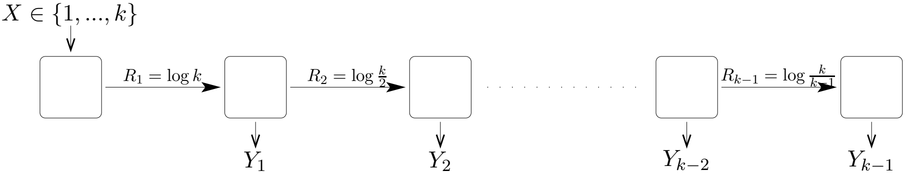



Optimal Communication:




$$
\begin{aligned}
R_{k-1} &= \log\left(\frac{k}{k-1}\right), \\
R_{k-2} &= \log\left(\frac{k}{k-1}\right) + \log\left(\frac{k-1}{k-2}\right) = \log\left(\frac{k}{k-2}\right), \\
R_i &= \log\left(\frac{k}{i}\right).
\end{aligned}
$$

# Cascade - One Assigned

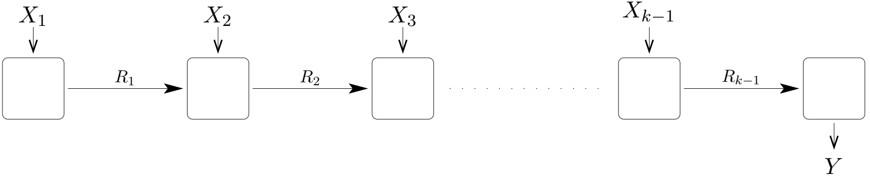



Sum rate:

$$
\begin{aligned}
R &= \sum_{i=1}^{k-1} \log\left(\frac{k}{i}\right) \\
&= k \log k - \sum_{i=1}^{k} \log i \\
&= k \log k - \log k! \\
&\approx k \log k - \log \left(\frac{k}{e}\right)^k \\
&= k \log e.
\end{aligned}
$$

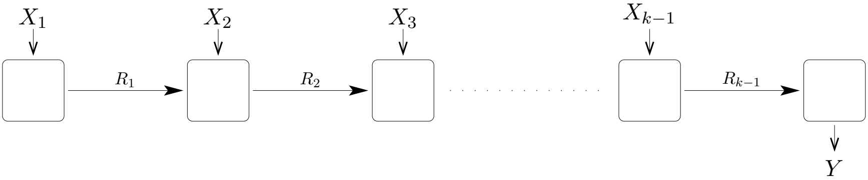
Linear in k

# Cascade - All But One Assigned (open problem)




$X_i$ unique in $\{1, ..., k\}$ for all $i$.
$Y$ must be the remaining task.

# Cascade - All But One Assigned (open problem)

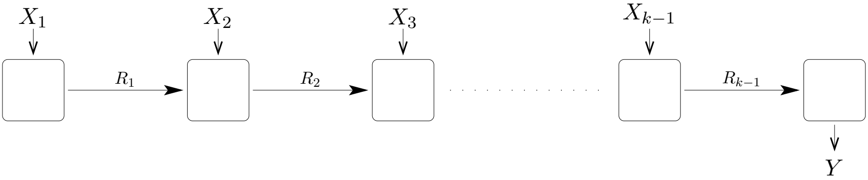



$X_i$ unique in $\{1, ..., k\}$ for all $i$.
$Y$ must be the remaining task.

Idea - Accumulate information:

$$\begin{aligned} R_1 &= \log(k-1), \\ R_2 &= \log(k-1) + \log(k-2) - \log 2, \\ R_i &= \log \binom{k-1}{i}. \end{aligned}$$

# Cascade - All But One Assigned (open problem)

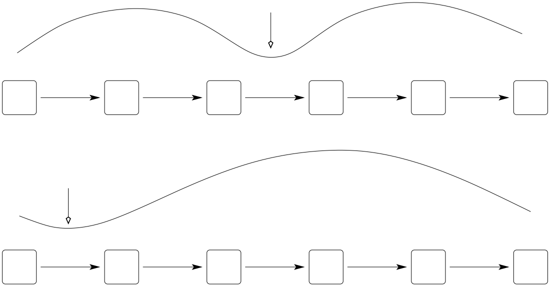



$X_i$ unique in $\{1, ..., k\}$ for all $i$.
$Y$ must be the remaining task.

Better Idea - Accumulate mod $k$ sum:

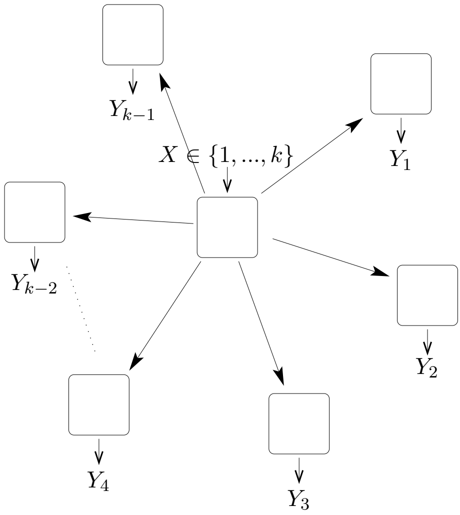
$$R_i \quad < \quad \log k, \text{ for all } i.$$

# Lower Bounds



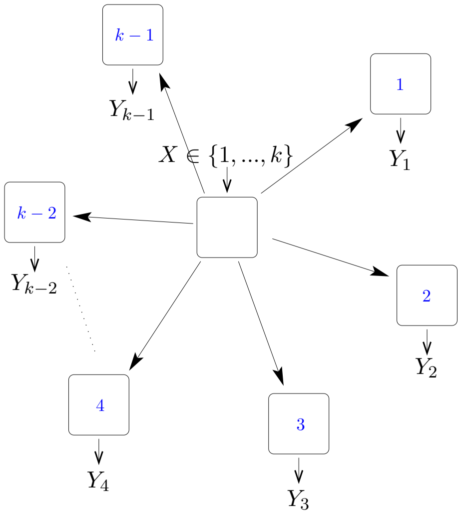
$$R_i \;\; \geq \;\; \log(i+1). \qquad\qquad \sum_{i=1}^{k-1} R_i \;\; \geq\approx \;\; k \log \frac{k}{e}.$$

# Star Network




Try $R_i = \log \frac{k}{k-1}$ for all $i$. (Doesn't work)

# Star Network

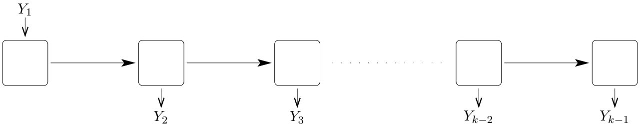



Try $R_i = \log \frac{k}{k-1}$ for all $i$. (Doesn't work)

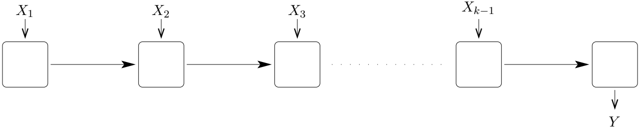
Assign Default Tasks: $R_i = h\left(\frac{1}{k}\right) \approx \frac{\log k}{k}$.

# Task Assignment Summary

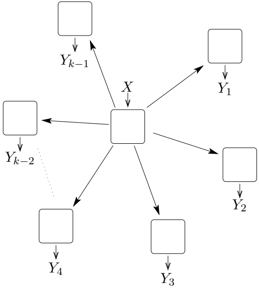
Sum rate:




$R_{min} \approx k \log e$ (linear)

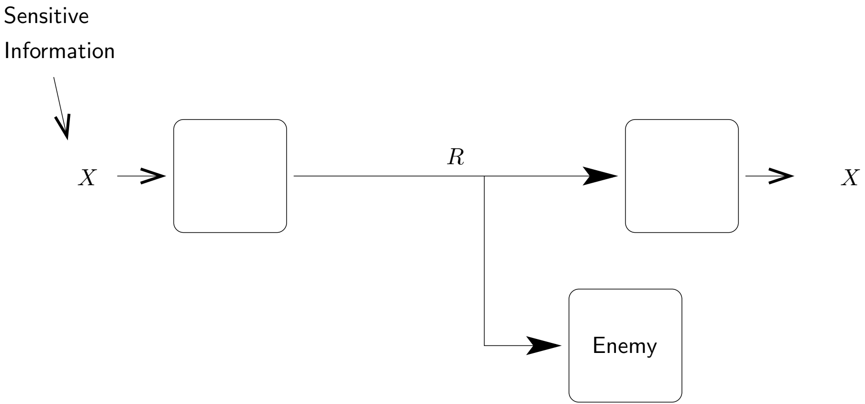



$$R_{min} \approx k \log k.$$

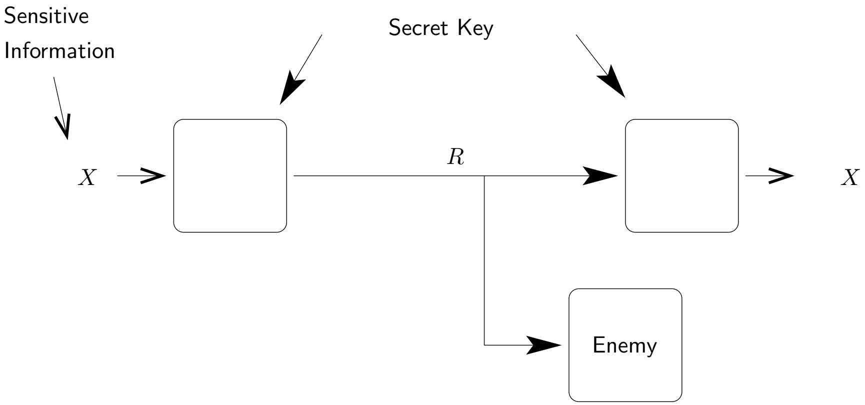



$$R_{min} \approx \log k.$$

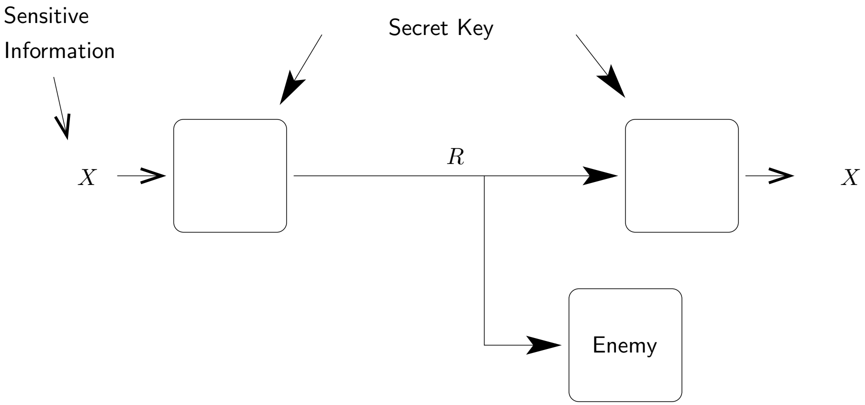
# Encryption



# Encryption



# Encryption




$$R_1 = R_2 = H(X).$$

# Game Theory

Why keep a secret?

How about Game Theory?

| | | Enemy 0 | Enemy 1 |
|---|---|---|---|
| Me $p(x)$ | 0 | 1 | 2 |
| | 1 | 3 | $-1$ |

# Game Theory

Why keep a secret?

How about Game Theory?

My team $p(x, y)$, Enemy

| | 0 | 1 |
|---|---|---|
| 00 | $1$ | $2$ |
| 01 | $3$ | $-1$ |
| 10 | $0$ | $1$ |
| 11 | $-1$ | $0$ |

# Team Action


Isolated Participants:

$$p(x)p(y)$$

# Team Action

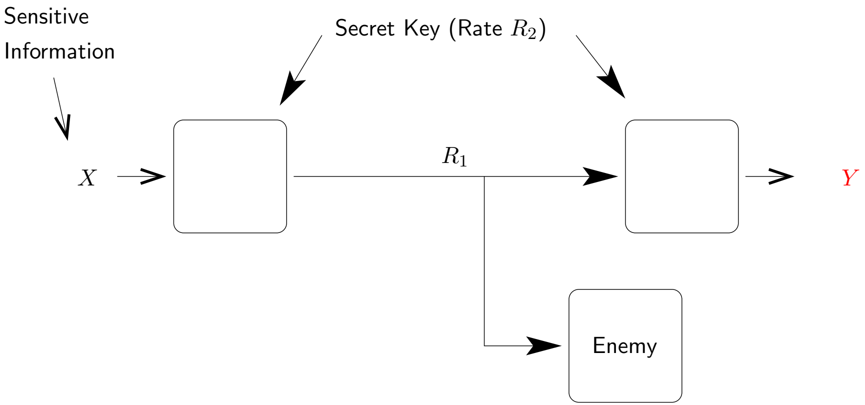

Isolated Participants:

$$p(x)p(y)$$

With Communication:

$$p(x, y)$$

# Relaxed Encryption




Goals:

1. $Y$ correlated with $X$ according to desired $p(y|x)$.
2. Enemy knows nothing about $X$ or $Y$.

# Relaxed Encryption Theorem

## Theorem

*For any source distribution $p_0(x)$ and any desired correlation $p(y|x)$:*

*Communication:*

$$R_1 \geq I(X;U).$$

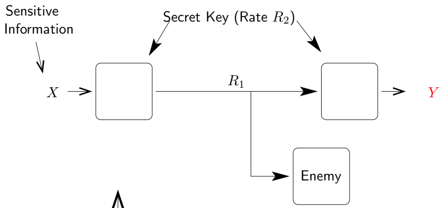
*Encryption:*

$$R_2 \geq I(X,Y;U).$$

*where $U$ is some random variable*
*that separates $X$ and $Y$ in the Markov sense.*
*(i.e. $X - U - Y$ form a Markov chain.)*

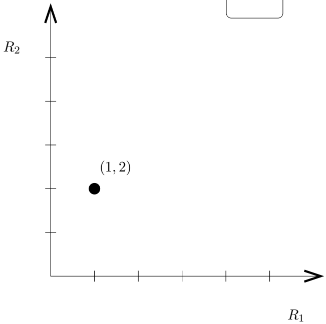
# Example

Task assignment in an adversarial setting.
Virus Scanner.



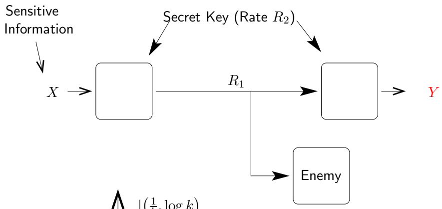

$X \sim Unif\{1, ..., k\}$.

$Y$ needs to be different from $X$ and **random among the choices**.



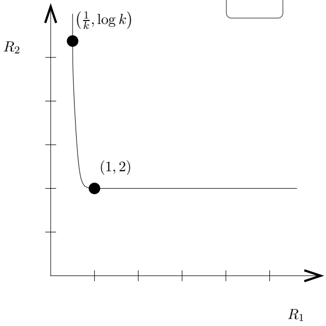
# Example

Task assignment in an adversarial setting.
Virus Scanner.

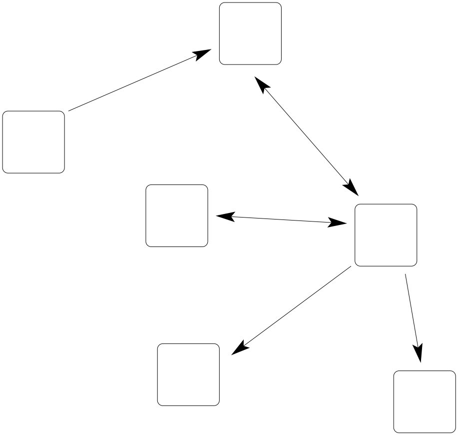



$X \sim Unif\{1, ..., k\}$.

$Y$ needs to be different from $X$ and **random among the choices**.



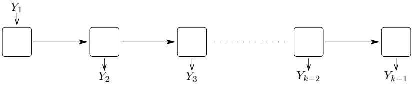
# Recap

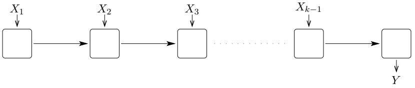


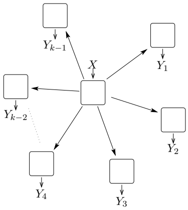
- Tools: Random coding, auxiliary variables, common randomness.
- Different networks require very different techniques.

# Summary

Non-adversarial:




Adversarial:

Two Nodes:

- Achieve Correlated $Y \sim p(y|x)$
- Secret key required
- Tradeoff between communication and secret key

Fundamental Limits:

- Communication: $R_1 > I(X;Y)$.
- Secret key: $R_2 > C(X;Y)$.

Game Theory Perspective for Encryption