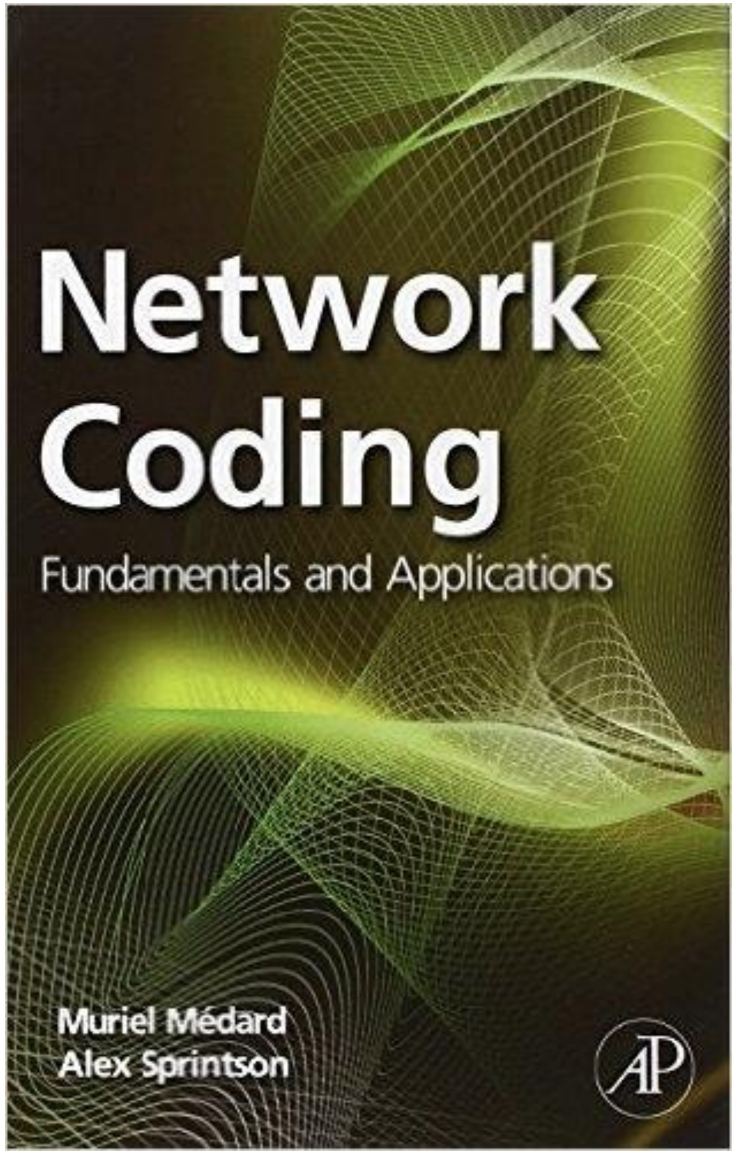
Network (Coding) Security:

Known knowns, Unknown knowns, and Unknowns

Sidharth Jaggi, The Chinese University of Hong Kong

Known knowns: Background



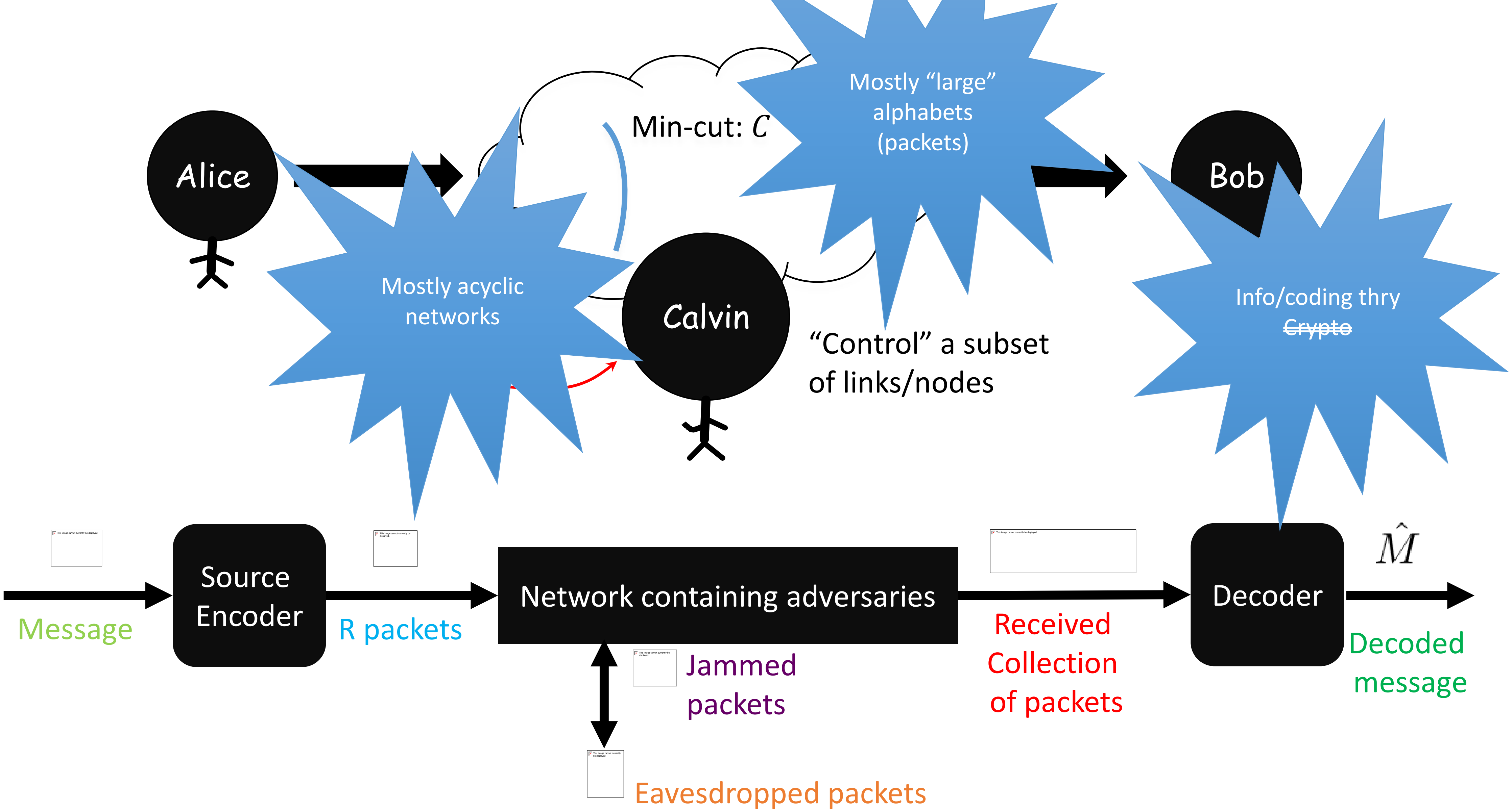
7. **Secure Network Coding: Bounds and Algorithms for Secret and Reliable Communications**
   Sidharth Jaggi and Michael Langberg

What is security?

The quality or state of being *secure*: as
a) : freedom from danger : safety
b) : freedom from fear or anxiety
c) : freedom from the prospect of being laid off

-Merriam-Webster

Background – Communication Scenario

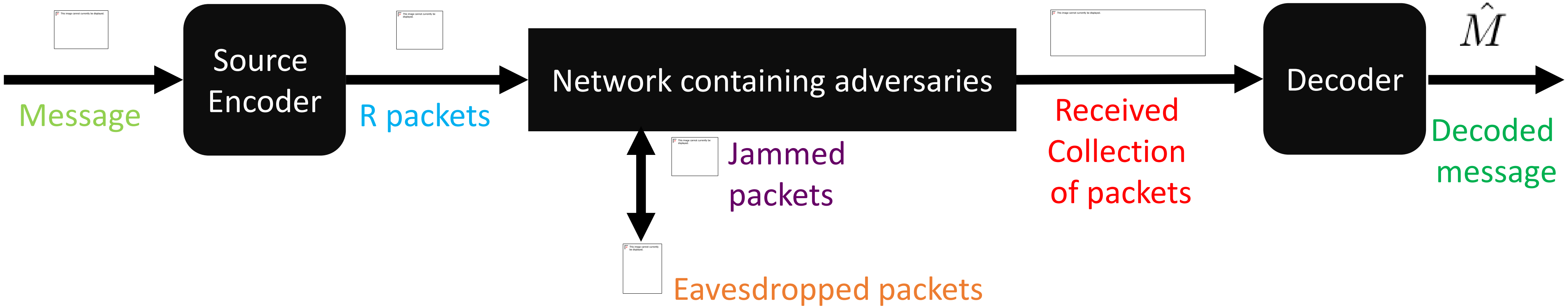


Background – Communication Scenario

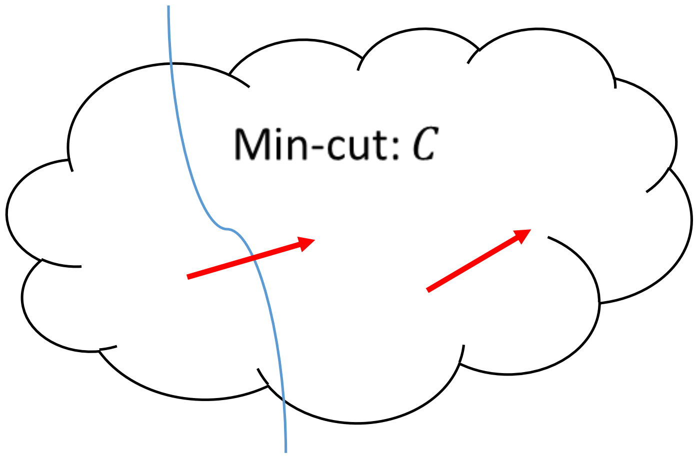
- Secrecy
- Robustness to erasures/ errors.

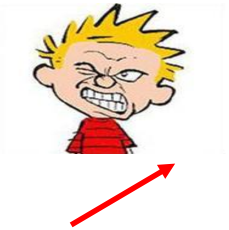
$$\Pr(\hat{M} \neq M) \approx 0$$

- More later…

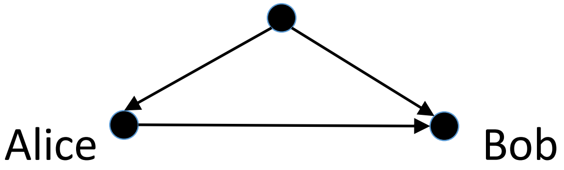


Secrecy





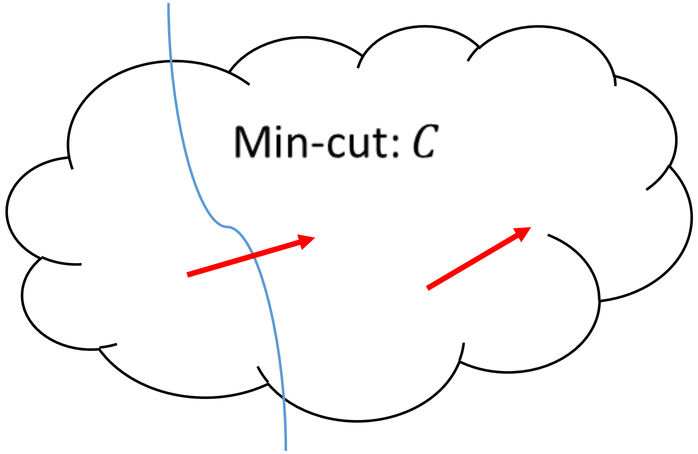
- Cai-Yeung: Secrecy rate $C\text{-}Z_r$ achievable (intuition – "network wiretap channel")
- Feldman et al: small field-sizes, random codes, efficient
- Silva et al: "Universal" codes (rank-metric/subspace codes)
- Multiple other works… Rouayheb et al, Bhattad et al, Ngai et al, …



- Cui et al – LP formulation that's never worse than $C\text{-}Z_r$
- General problem still open
- Node eavesdropper problem even harder

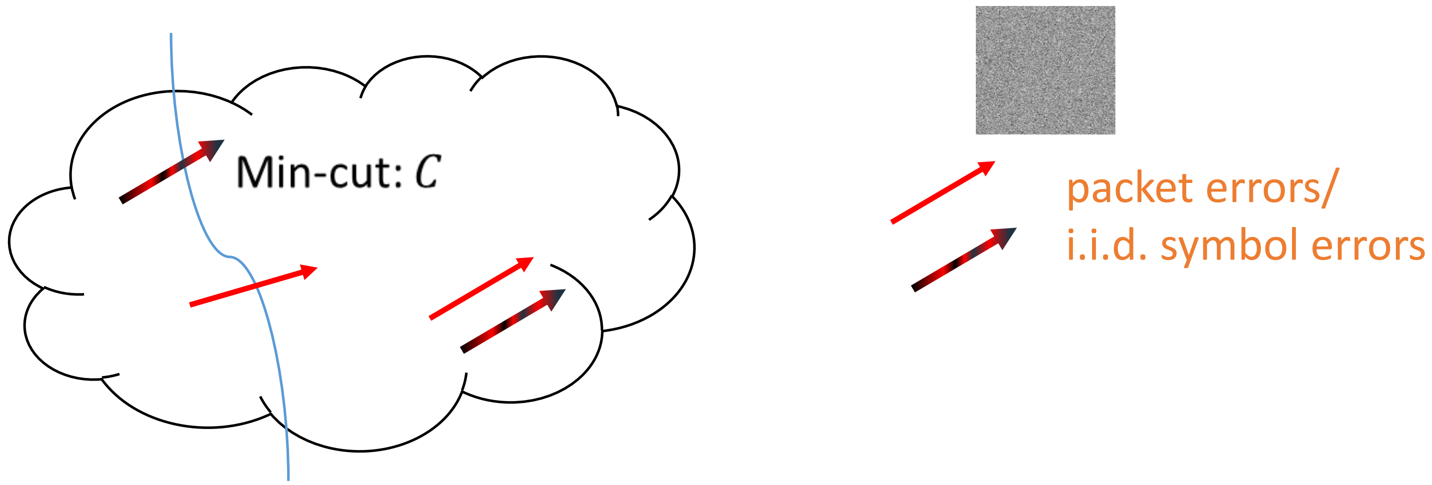
$C=1$, $Z_r=1$,
but secrecy rate 1 possible!

Erasures



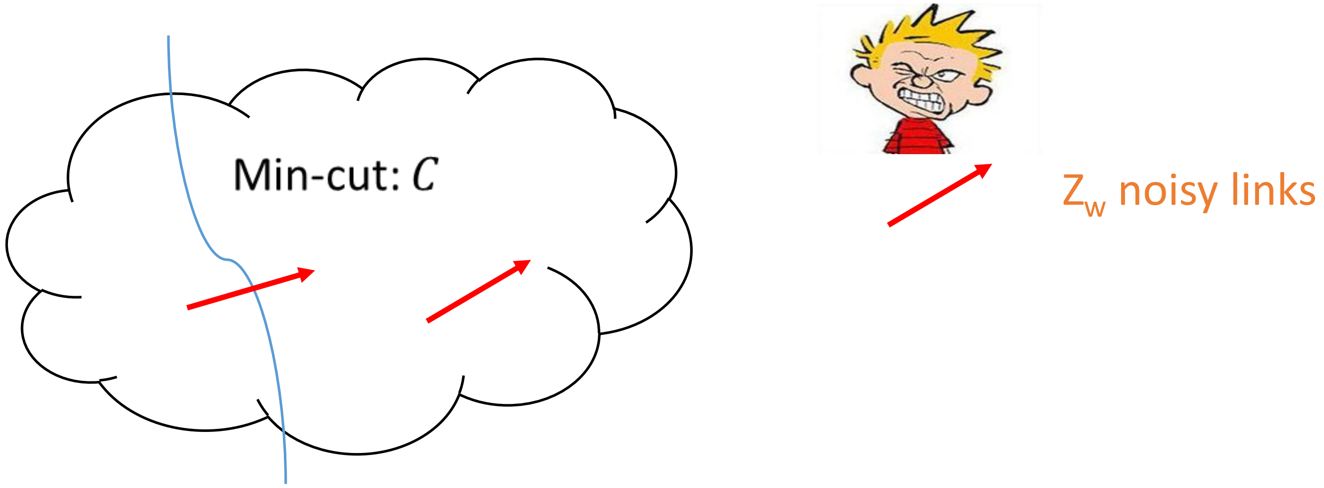
- Kötter-Médard: Rate C-Z_w possible. Optimal.
- Ho et al: expected throughput for random erasures, efficient random distributed codes
- Dana et al: Even correlated random erasures (interference) rate computable, efficiently attainable
- Silva et al: Rank-metric codes for worst-case erasures
- Node-erasures: Capacity based on node-cut attainable

“Random” Error-correction



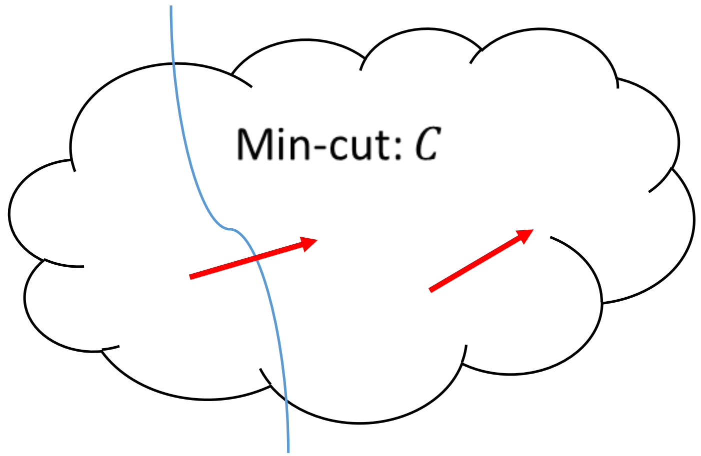
- Song et al/Borade et al: Symbol errors: Separation between link-by-link error-correction/network coding
- Silva et al: Rate $C\text{-}Z_w$ efficiently attainable end-to-end with random packet errors (rank-metric codes)

Error-detection



- Omniscient Calvin: Rate $R < C-Z_w$ possible with error-detection. Optimal.
- Ho et al: Any rate, at least one-path Calvin does not control (see/jam), can detect errors. Optimal.

Adversarial errors



- Cai-Yeung: Rate C-2Z_w possible. Optimal. Network Singleton bound/Network GV codes
- Jaggi et al/Kötter-Kschischang/Kötter-Kschischang-Silva: Efficient codes achieving C-2Z_w
- Jaggi et al: If Calvin not omniscient, C-Z_w possible in some scenarios (more on this later)
- Node adversary problem much harder (more on this later).

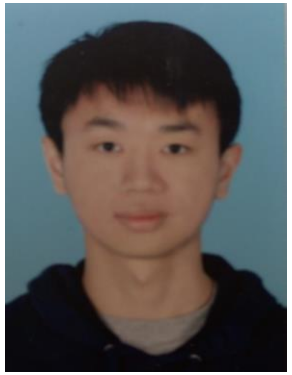
Addenda …

- Cryptography (computational assumptions)
- List-decoding
- Rateless codes
- …

Unknown knowns part I:

Reliable and Secure Communication over Adversarial Multipath Networks

Codes, Algorithms, Networks: Design & Optimization in Information Theory



Qiaosheng Zhang Eric

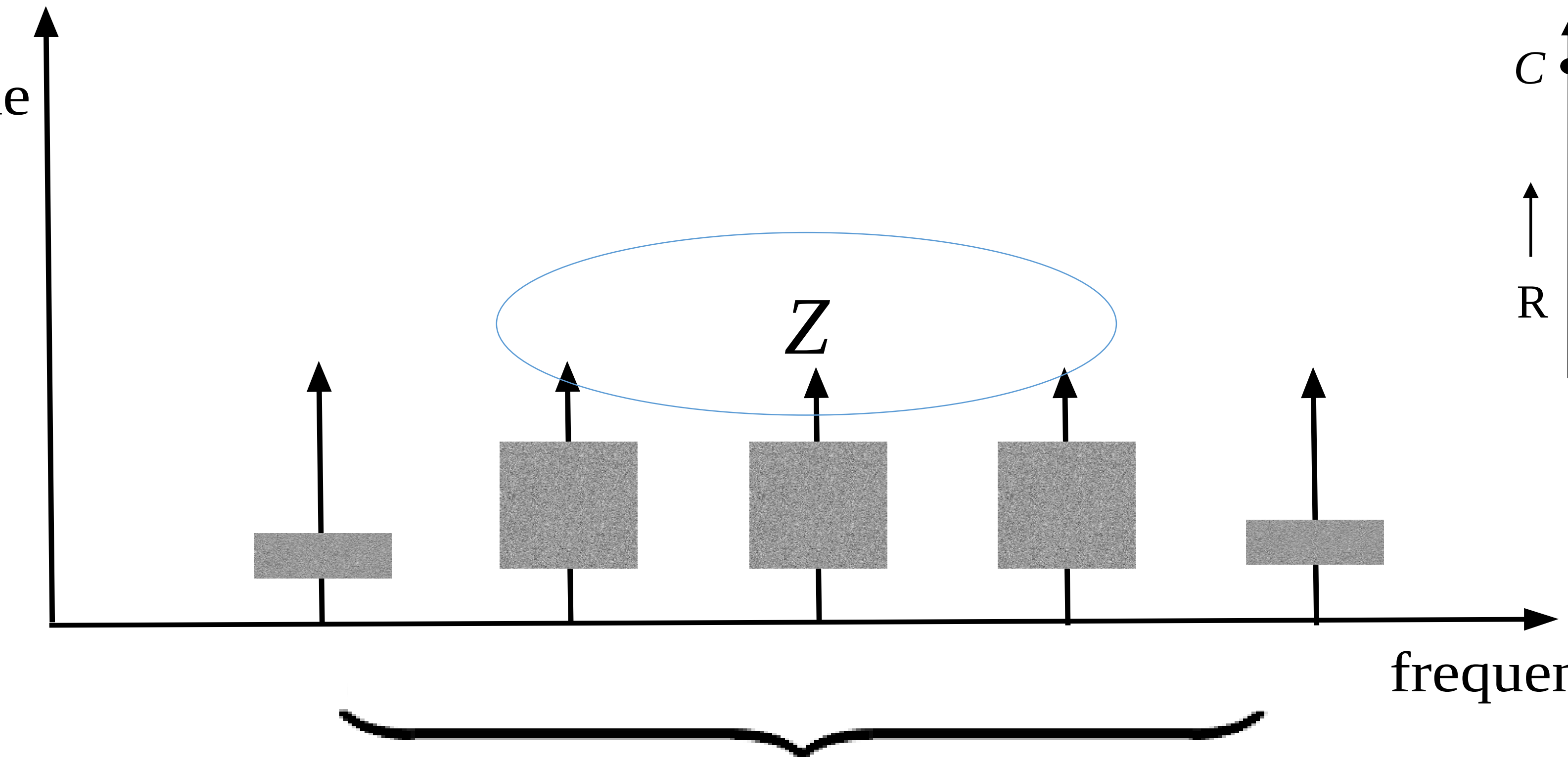
Mayank Bakshi

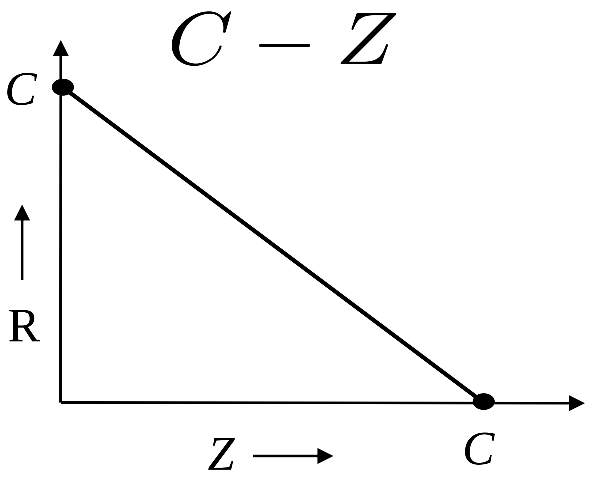
Sidharth Jaggi

Swanand Kadhe

Alex Sprintson

Motivating Example 1



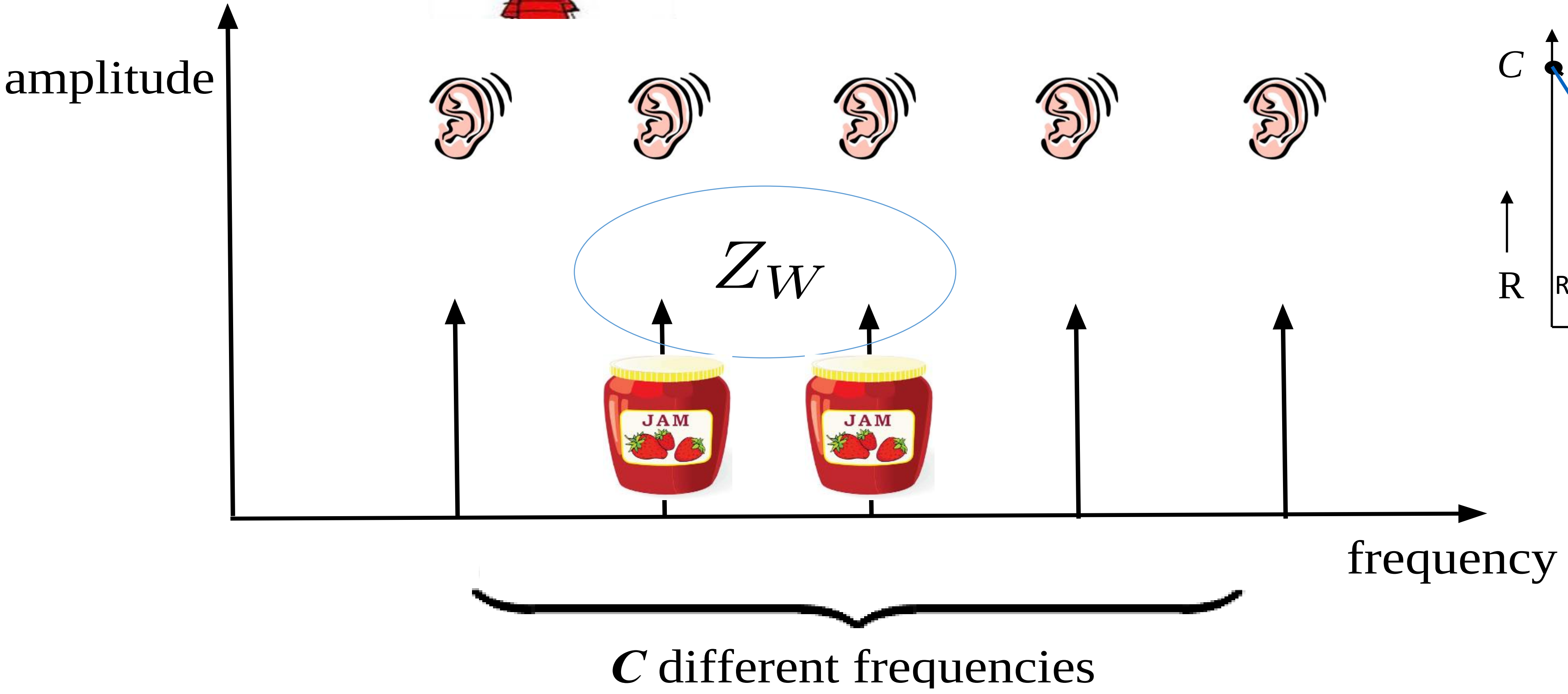


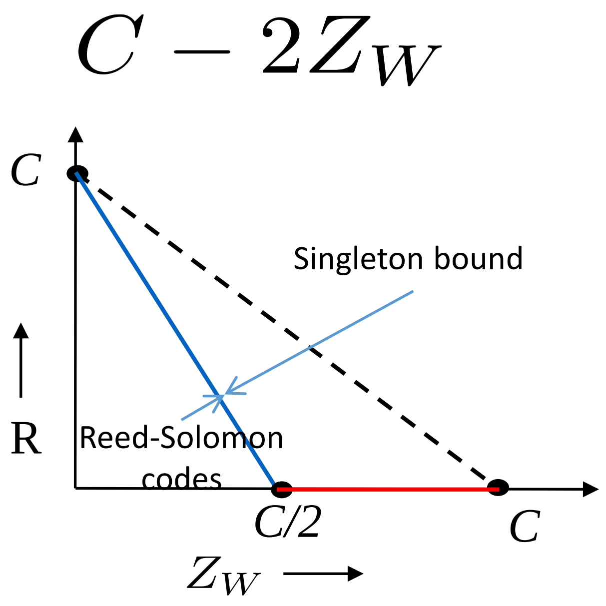
Alice

Bob

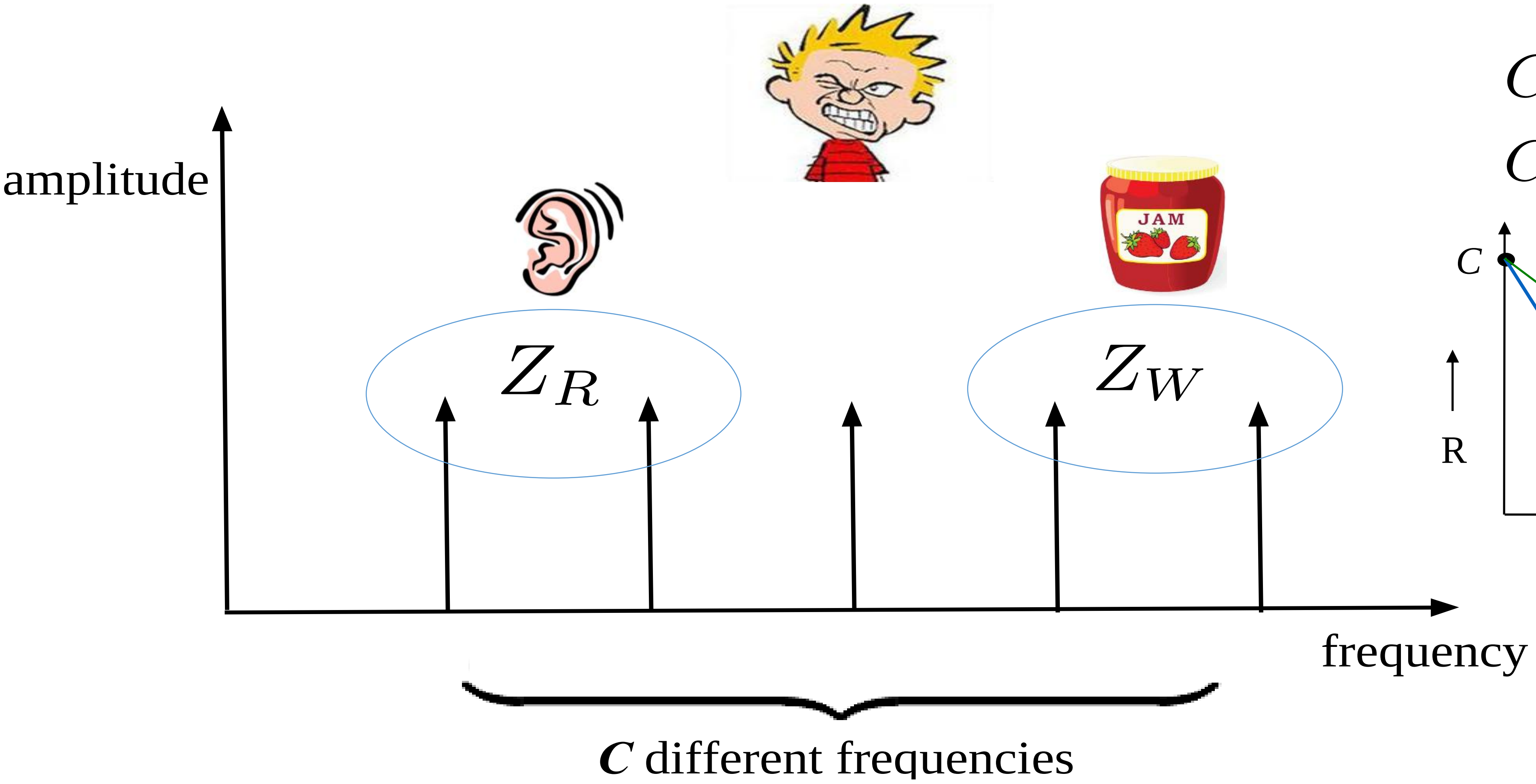
Motivating Example 2

Eavesdrops on all the frequencies

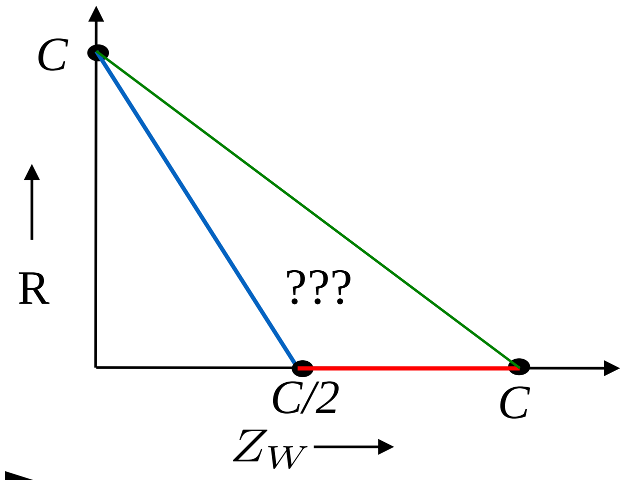




Motivating Example 3



$$C - Z_W$$
$$C - 2Z_W$$



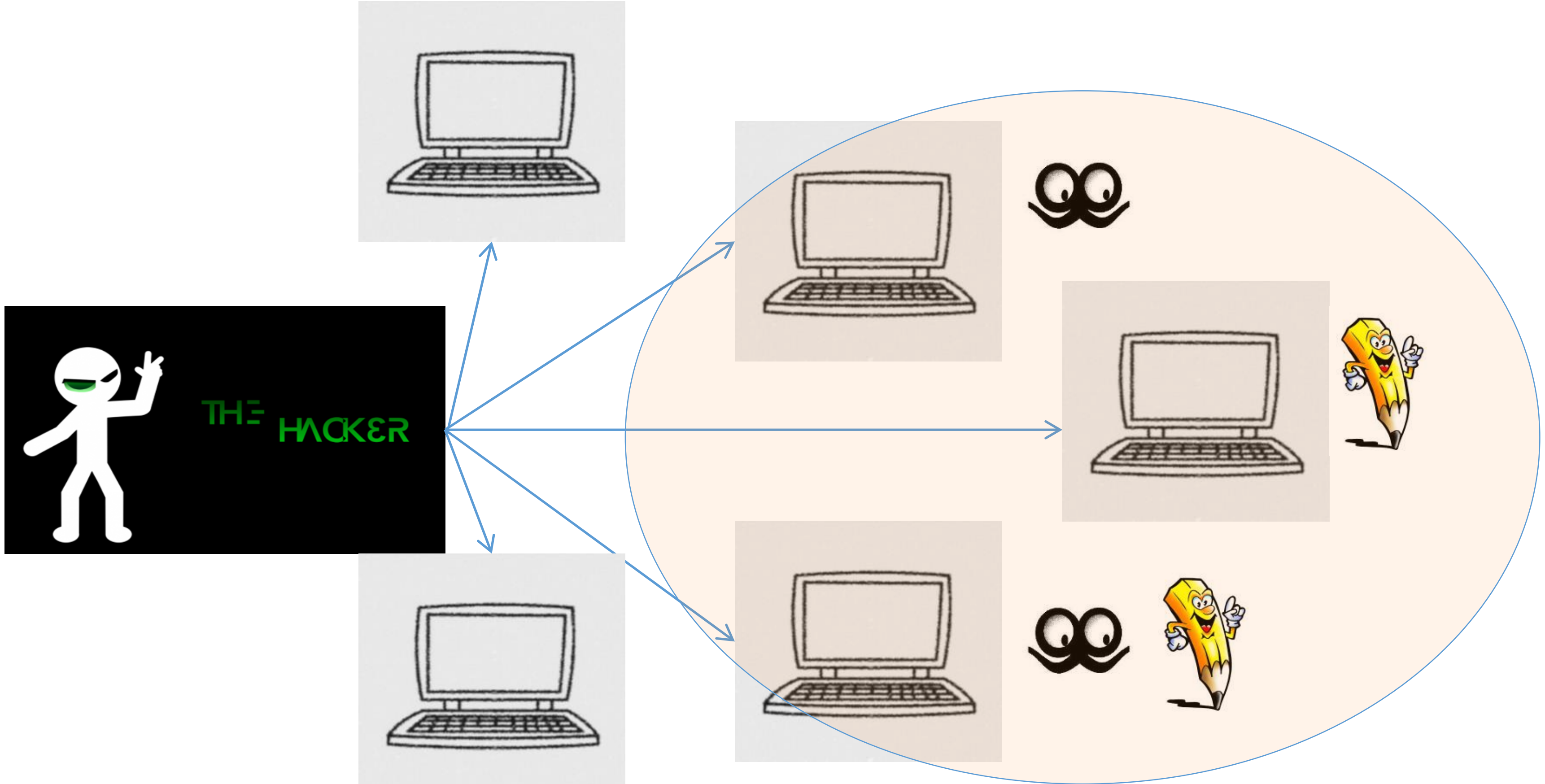
Alternate Motivation

- ***C*** computers
- Administrator: wants to store a file.
  - How? By distributing it across ***C*** computers.

1 2 3 ***C***

Alternate Motivation

- Administrator: wants to store a file.
  - But hacker has read/write privileges on some servers…



Alternate Motivation

- **Goals:**

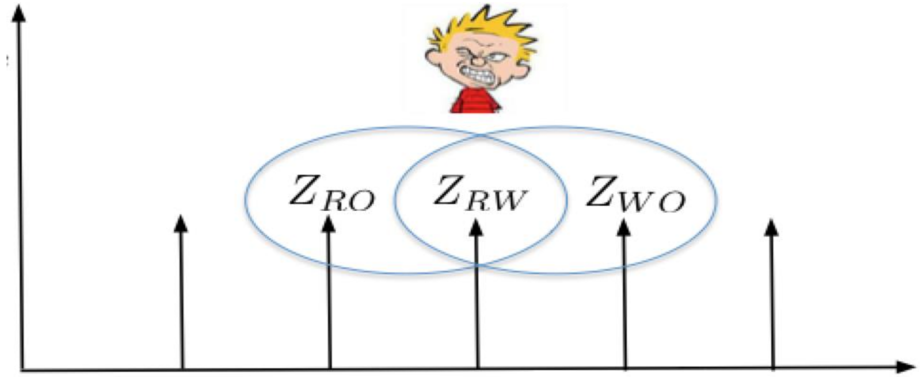
(1) The hacker cannot corrupt the file

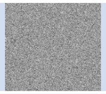
------ reliability

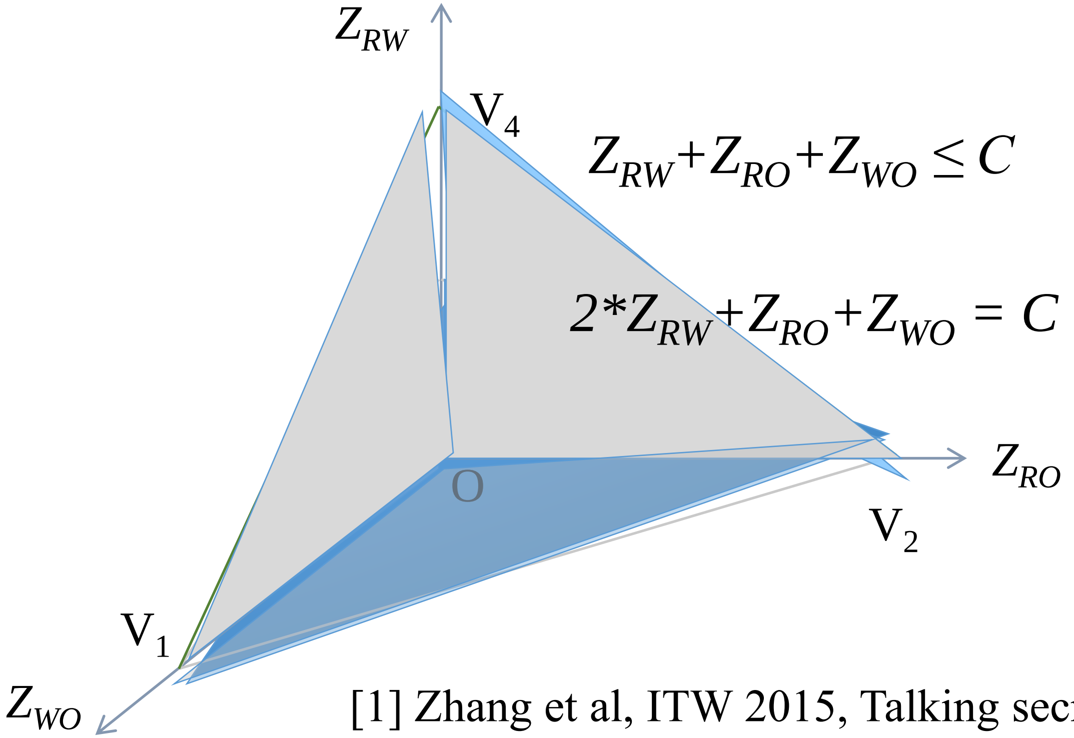
(2) The hacker cannot decipher the contents.

------ secrecy

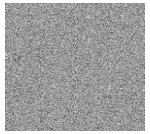
Basic model



Optimal rate	Regime
$C - Z_{RW} - Z_{WO}$ 	***Weak*** adversary regime
$C - \mathbf{2}{*}Z_{RW} - Z_{WO}$ 	***Strong*** adversary regime



- ***Strong*** adversary regime:
  Tetrahedron $V_1V_2V_3V_4$



- ***Weak*** adversary regime:
  Tetrahedron $OV_1V_2V_3$

[1] Zhang et al, ITW 2015, Talking secretly, reliably and efficiently: A "complete" characterization

Basic model

- Non-causal condition (Model 0) ⟷ One-shot transmission

x_1	x_1
x_2	y_2
x_3	x_3

[1] Zhang et al, ITW 2015, Talking secretly, reliably and efficiently: A “complete” characterization

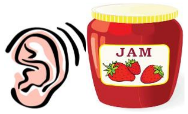
Causality/feedback

- Effect of *causality* ? (Model 1)
  - Cannot see the future
  - Stuck to fixed channels

ONE-SHOT TRANSMISSION
MULTI-ROUND TRANSMISSION

x_1		
x_{23}	x_{22}	x_{21}
x_{33}	x_{32}	x_{31}

x_{13}	x_{12}	x_{11}
y_{23}	y_{22}	y_{21}
x_{33}	x_{32}	x_{31}



Causality/feedback

- Effect of *passive feedback* ? (Model 2)

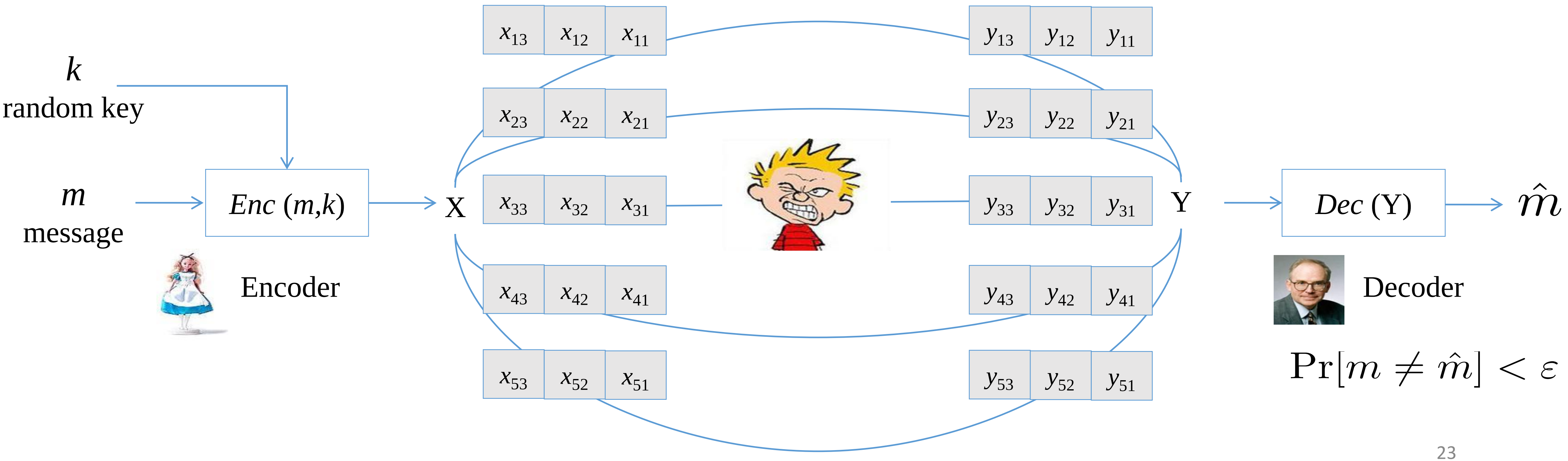
x_{13}	x_{12}	x_{11}
x_{23}	x_{22}	x_{21}
x_{33}	x_{32}	

x_{12}	x_{11}
y_{22}	y_{21}
x_{32}	x_{31}

x_{13}	x_{12}	x_{11}
y_{23}	y_{22}	y_{21}
x_{33}	x_{32}	x_{31}

Problem Statement

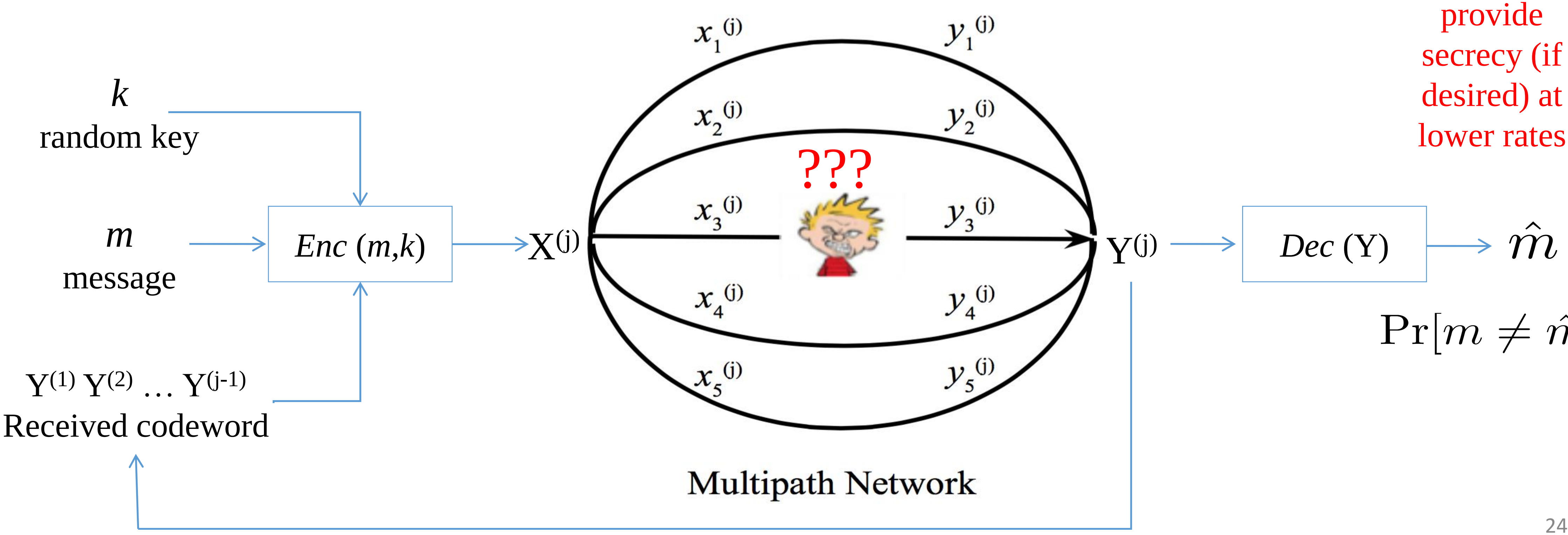
- **Multi-round transmission without feedback (Model 1)**
  - System diagram:



Problem Statement

- **Multi-round transmission with passive feedback (Model 2)**
  - System diagram: *j-th* round, $j = 1, 2, \ldots$

Can also provide secrecy (if desired) at lower rates

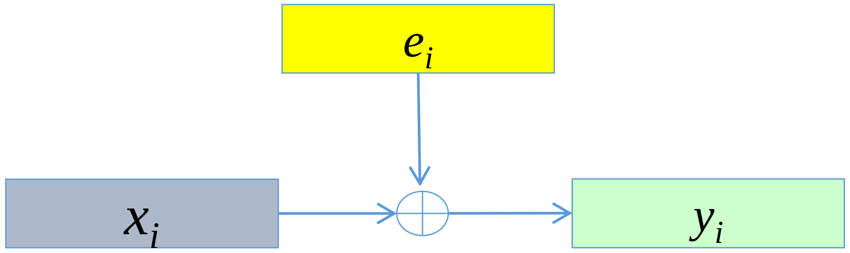


$$\Pr[m \neq \hat{m}] < \varepsilon$$

Jamming models

- Additive Jamming:

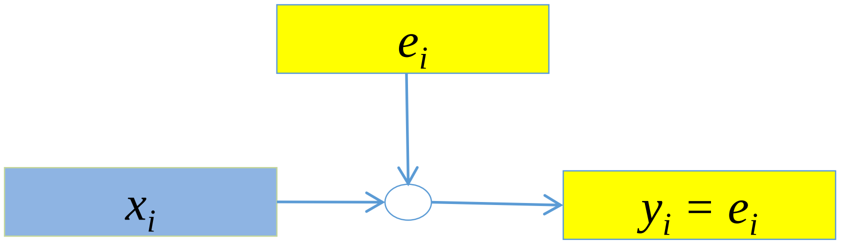
$$y_i = x_i + e_i$$



(Wireless network)

- Overwrite Jamming:

$$y_i = e_i$$



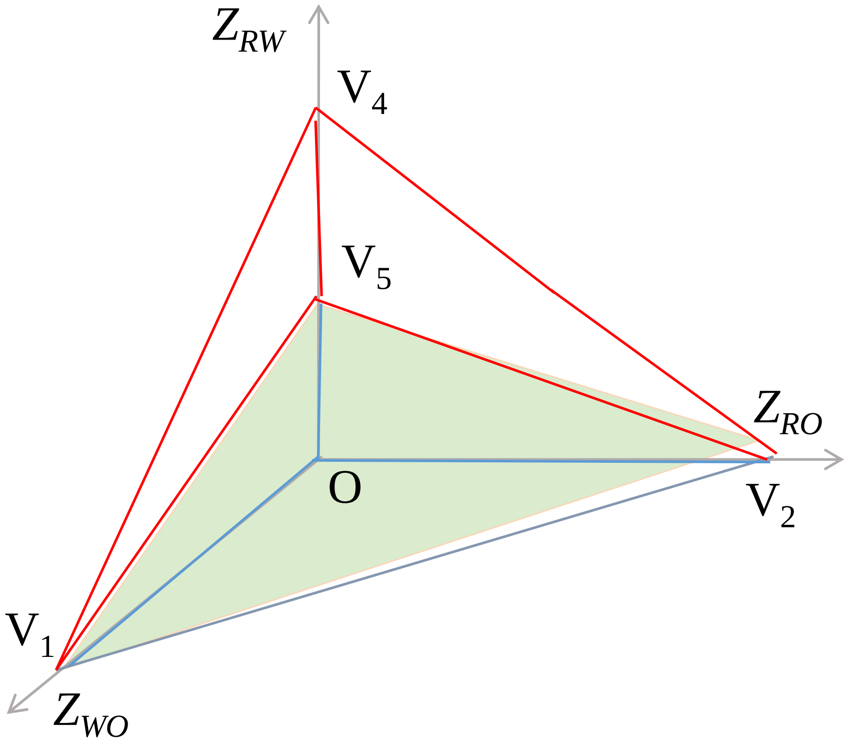
(Wired network / Storage system)

Results: A "Complete" Characterization

Model		regime	reliability	reliability & secrecy
Non-causal	additive	$z_{ro}+z_{wo}+2z_{rw}<C$	$C-(z_{rw}+z_{wo})$ $\hat{C}-(\Lambda_{z_{rw}+z_{wo}})_{max}$	$(C-z_{ro}-z_{wo}-2z_{rw})^+$?
		$z_{ro}+z_{wo}+2z_{rw}\geq C$	$(C-2z_{rw}-z_{wo})^+$ $(\hat{C}-(\Lambda_{2z_{rw}+z_{wo}})_{max})^+$	0 ?
	overwrite	$z_{ro}+2z_{wo}+2z_{rw}<C$	$C-(z_{rw}+z_{wo})$ $\hat{C}-(\Lambda_{z_{rw}+z_{wo}})_{max}$	$(C-z_{ro}-z_{wo}-2z_{rw})^+$?
		$z_{ro}+2z_{wo}+2z_{rw}\geq C$	$(C-2z_{rw}-2z_{wo})^+$ $(\hat{C}-(\Lambda_{2z_{rw}+2z_{wo}})_{max})^+$	0 ?
Causal w/o feedback	additive	$z_{wo}+2z_{rw}<C$	$C-(z_{rw}+z_{wo})$ $\hat{C}-(\Lambda_{z_{rw}+z_{wo}})_{max}$	$(C-z_{ro}-z_{wo}-2z_{rw})^+$
		$z_{wo}+2z_{rw}\geq C$	0	0
	overwrite	$2z_{wo}+2z_{rw}<C$	$C-(z_{rw}+z_{wo})$ $\hat{C}-(\Lambda_{z_{rw}+z_{wo}})_{max}$	$(C-z_{ro}-z_{wo}-2z_{rw})^+$
		$z_{wo}+2z_{rw}\geq C$	0	0
Causal with passive feedback	additive	$\{z_r=C \text{ and } 2z_w<C\}\bigcup\{z_r<C\}$	$C-(z_{rw}+z_{wo})$	$\min\{C-z_r, C-z_w\}$
		$z_r=C$ and $2z_w\geq C$	0	0
	overwrite	$z_{ro}+z_{wo}+z_{rw}<C$	$C-(z_{rw}+z_{wo})$	$(C-z_{ro}-z_{wo}-z_{rw})^+$
		$z_{ro}+z_{wo}+z_{rw}=C$	$(C-2z_{wo}-2z_{rw})^+$	0

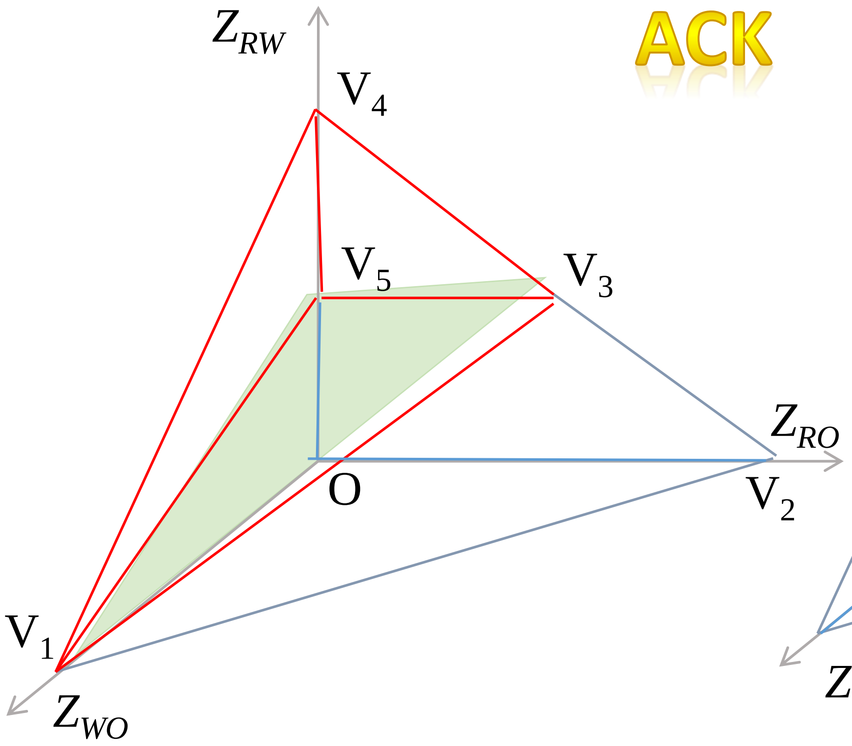
Overview of main results (*additive*)

BASIC MODEL

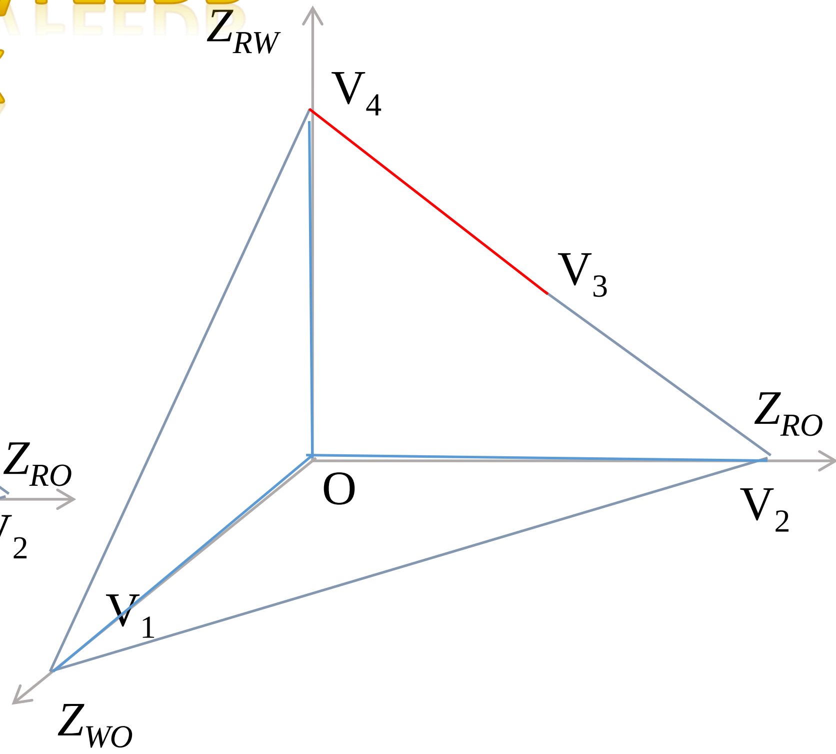


One-shot transmission
(Model 0)

CAUSALITY/FEEDBACK



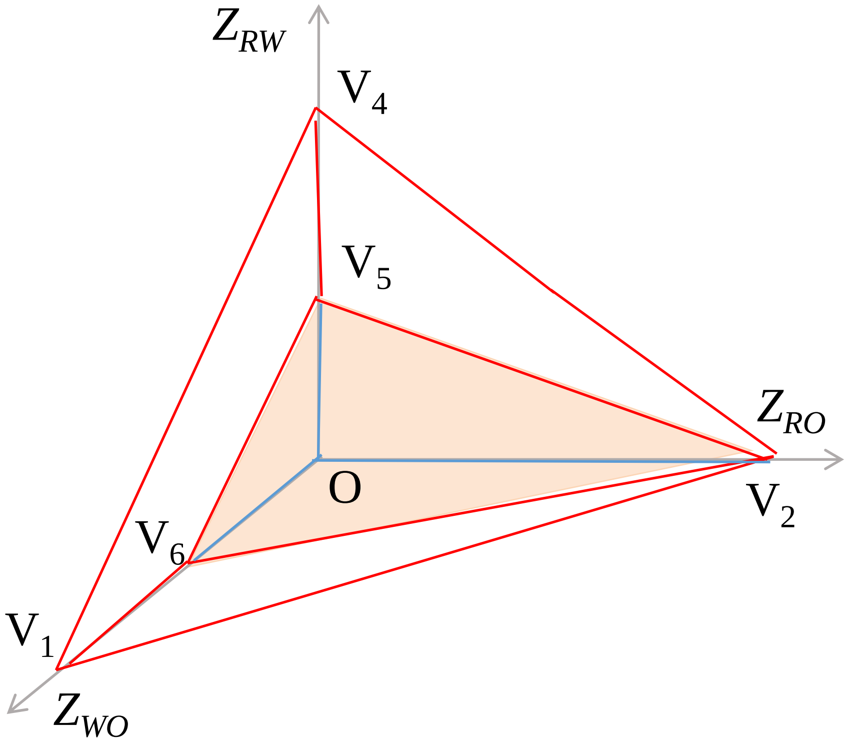
Multi-round transmission
Without feedback
(Model 1)



Multi-round transmission with Passive feedback
(Model 2)

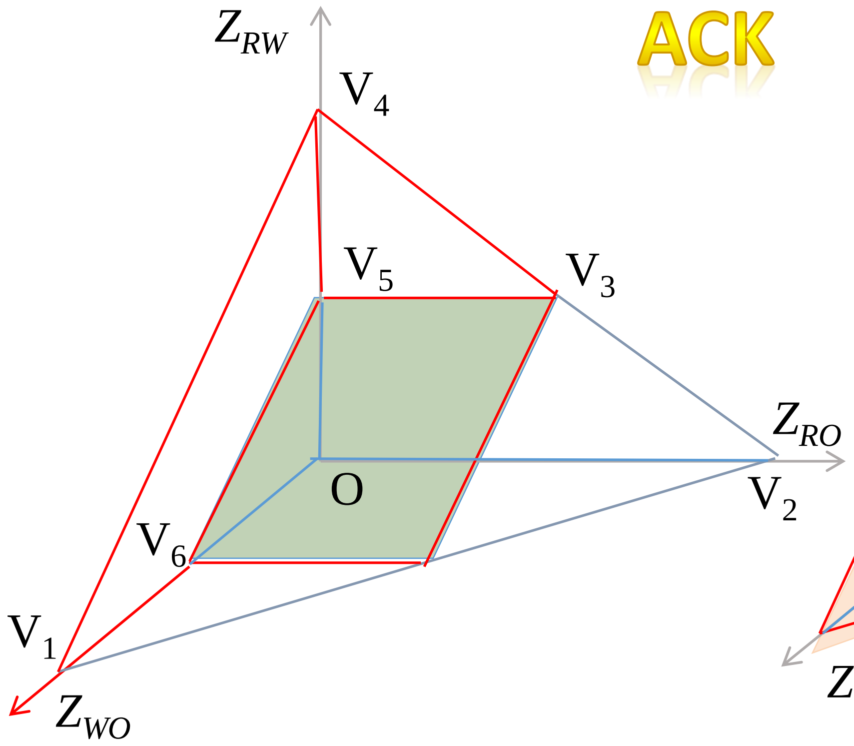
Overview of main results (*overwrite*)

BASIC MODEL

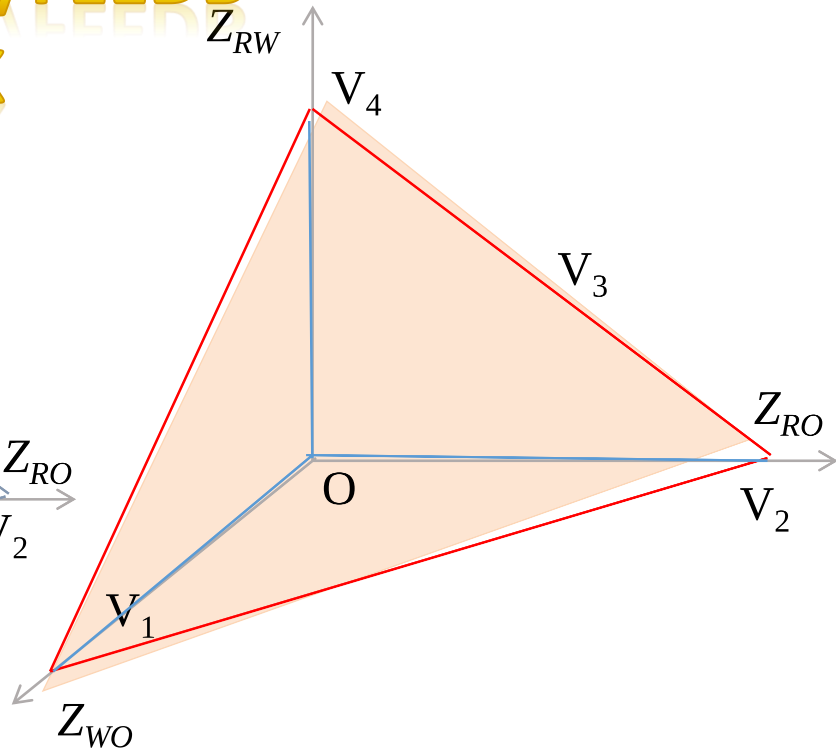


One-shot transmission
(Model 0)

CAUSALITY/FEEDBACK



Multi-round transmission
Without feedback
(Model 1)



Multi-round transmission with Passive
feedback
(Model 2)

Multi-round transmission without feedback (*additive*)

- Key idea for achievability:
  - *Self-hashing*
  - *Pairwise-hashing* [Jag06]

HASHING

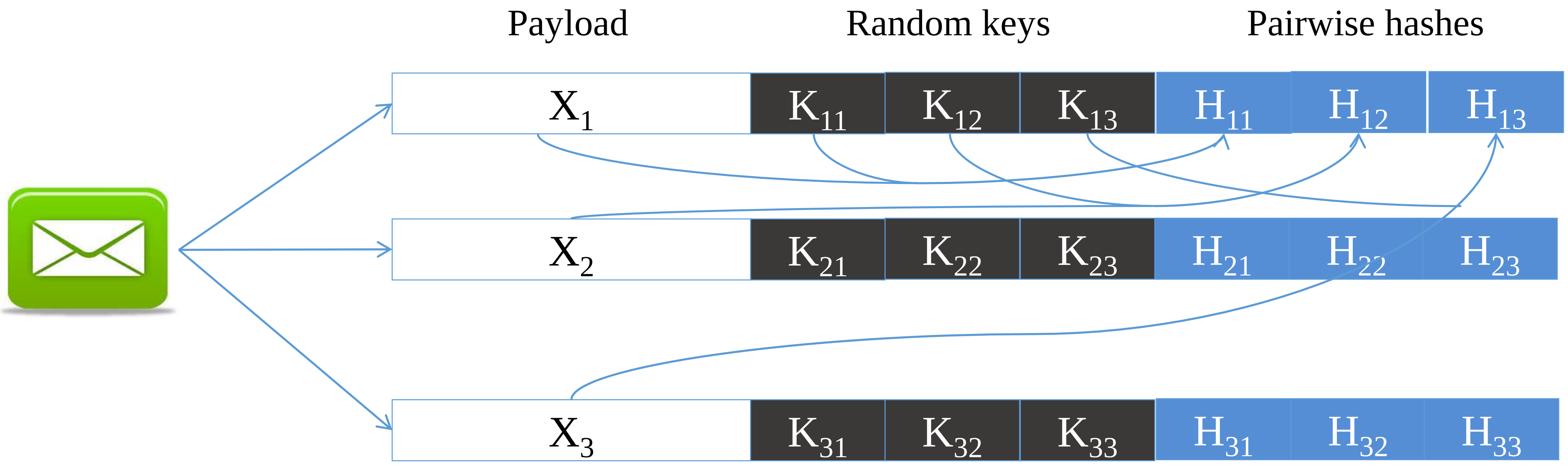
Y_i	K_i'	H_i'

Z_{WO}

Multi-round transmission without feedback (*additive*)

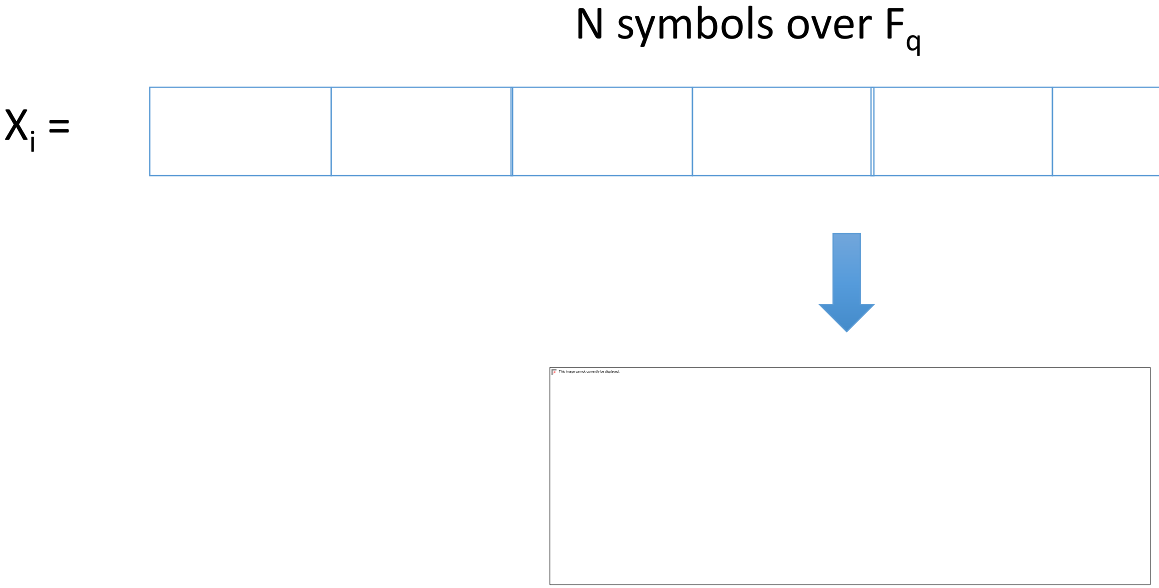
- Key idea for achievability:
  - *Self-hashing*
  - *Pairwise-hashing* [Jag06]

HASHING



Pairwise-hashing

- What's the hash function?



"Linearized polynomial"
(p ➔field characteristic)

Key idea for achievability: Pairwise-hashing [Jag06]

- Case 1:

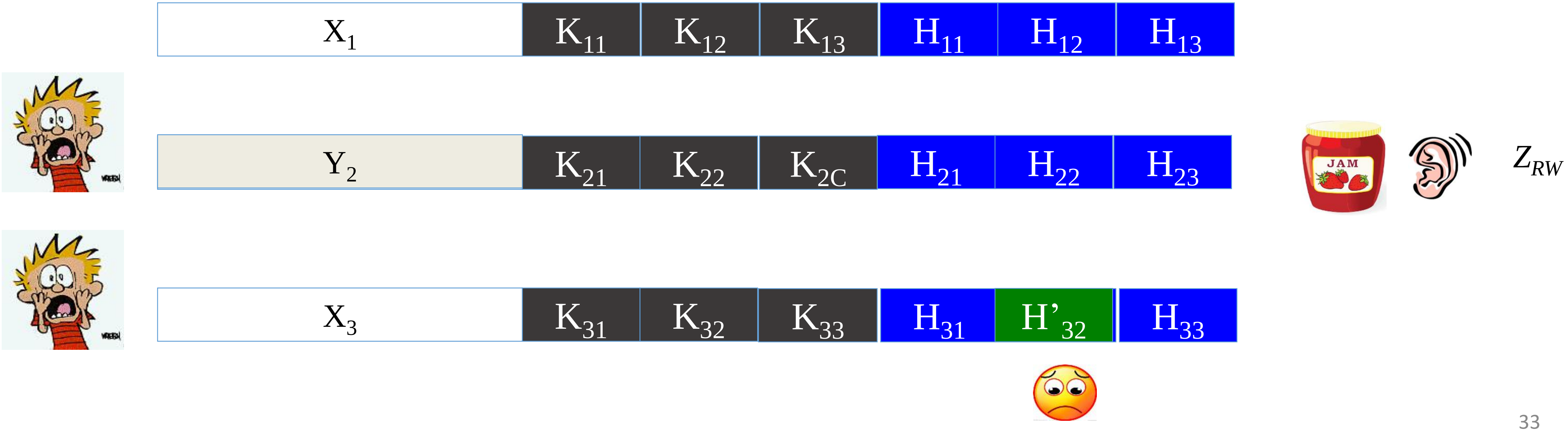
Link 1 and Link 2 are pairwise-consistent

X_1	K_{11}	K_{12}	K_{13}	H_{11}	H_{12}	H_{13}
X_2	K_{21}	K_{22}	K_{23}	H_{21}	H_{22}	H_{23}
X_3	K_{31}	K_{32}	K_{33}	H_{31}	H_{32}	H_{33}

Key idea for achievability: Pairwise-hashing [Jag06]

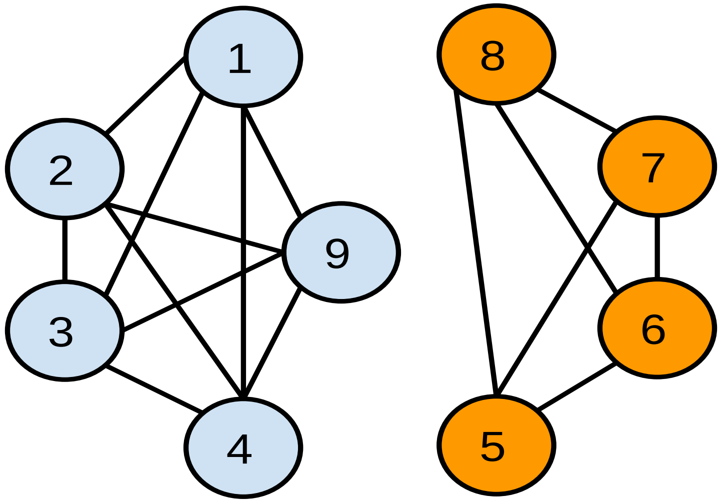
- Case 2:

Link 2 and Link 3 are not pairwise-consistent



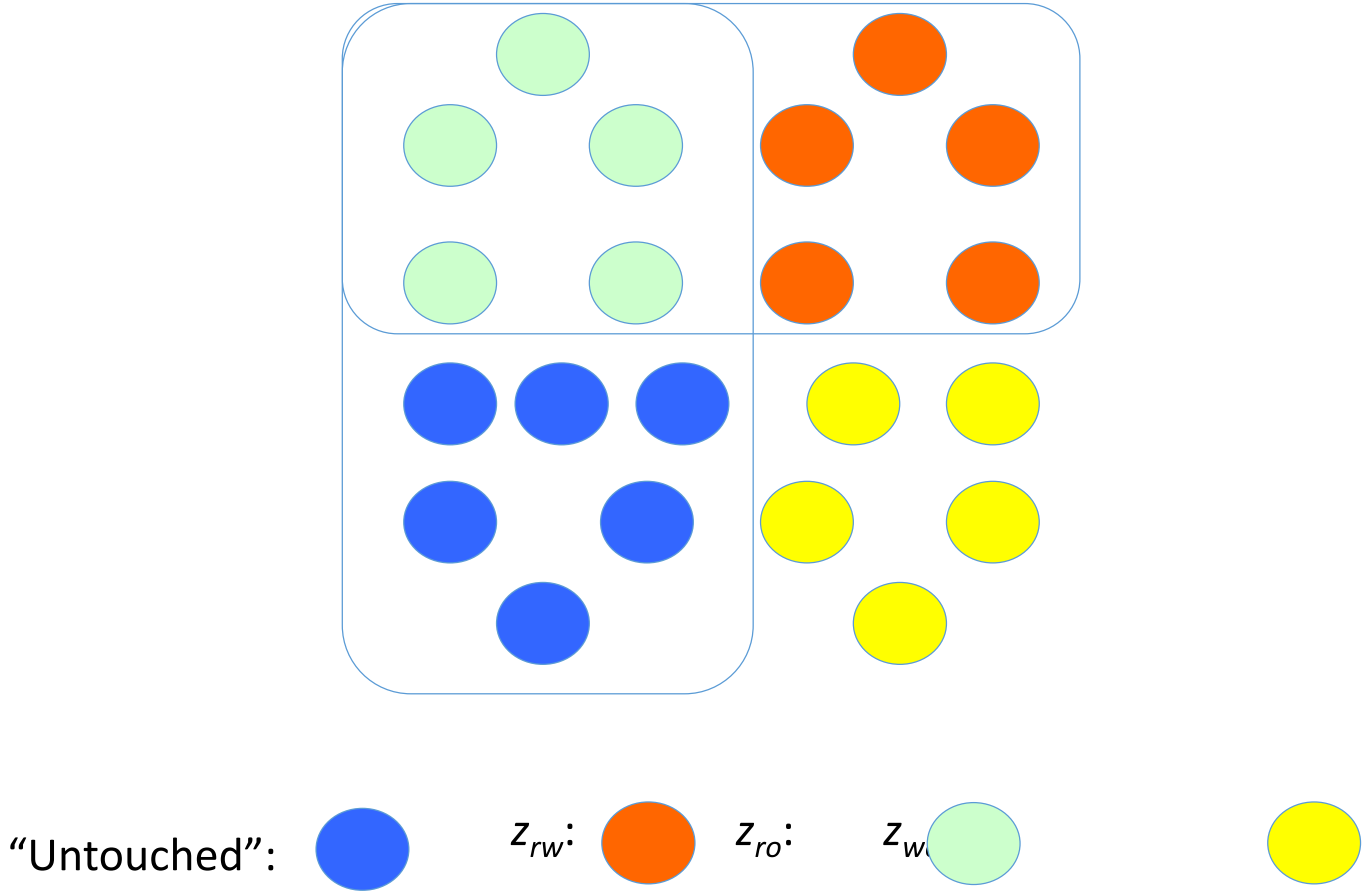
Pairwise-hashing Analysis

- Receiver Bob:
  - Construct a graph with C vertices.
  - Connect two vertices *if* consistent.
  - Find the largest clique (count node-degree).



Main Results

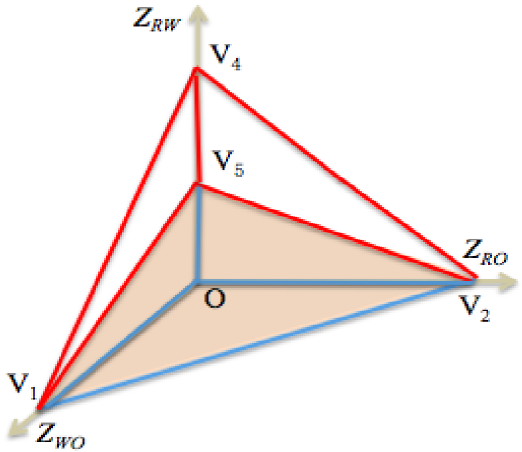
- <u>Eg: Additive Jamming:</u>
  - Calvin's clique:
    - $z_{rw} + z_{ro}$
  - Encoder's clique:
    - $C - z_{rw} - z_{wo}$

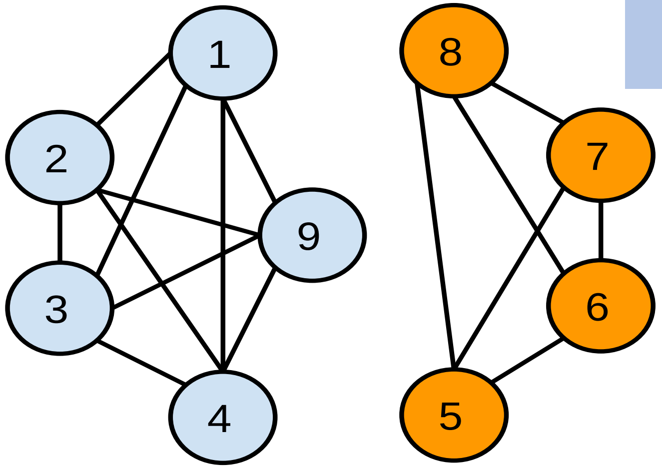


Key idea for achievability: Pairwise-hashing [Jag06]

- Decoder:
  - Check *pairwise-consistency*:
  - Errors are detectable if
    - $C - z_{rw} - z_{wo} > z_{rw} + z_{ro}$
    - $R = C - z_{rw} - z_{wo} = C - Z_W$

 	**Yes**	**No**
Yes	Z_{RW}	Z_{RO}
No	Z_{WO}	G

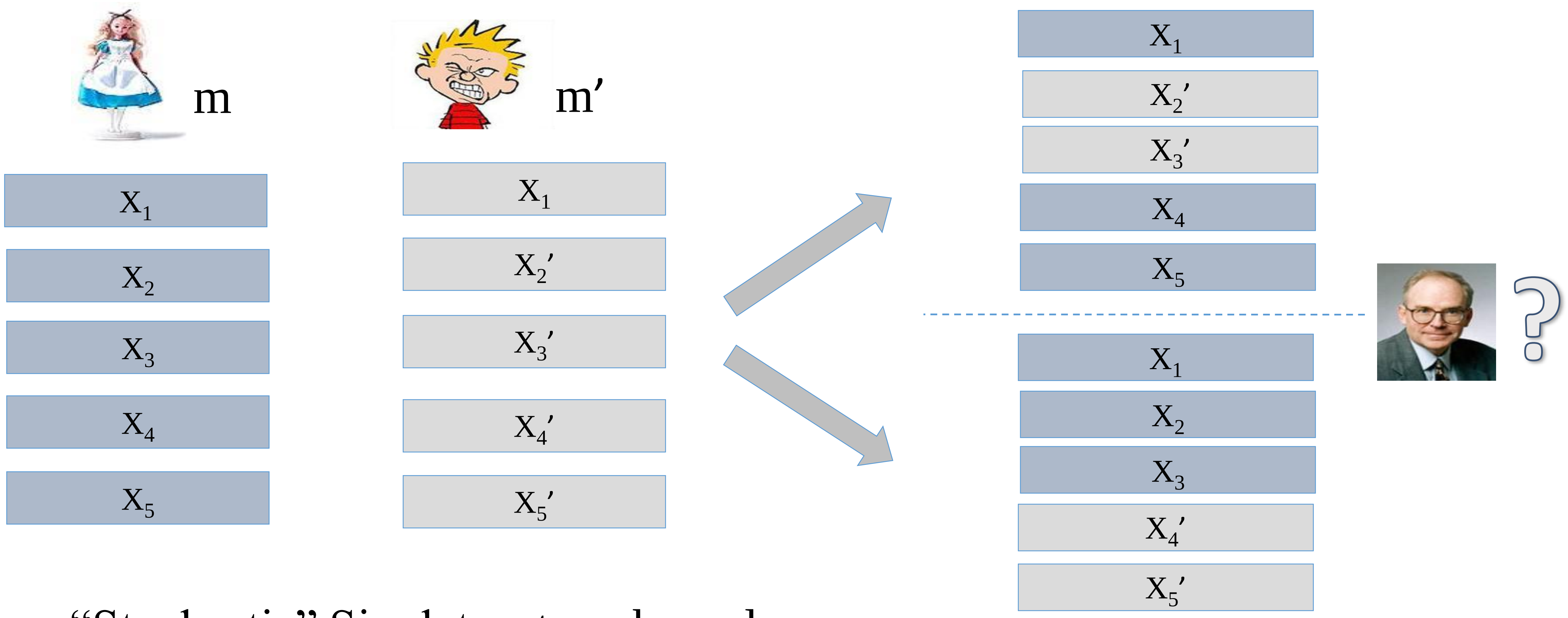




Converse: “Stochastic” symmetrization

Eg: Overwrite, $C=5$, $Z_{ro}=1$, $Z_{wo}=2$, $Z_{rw}=0$,

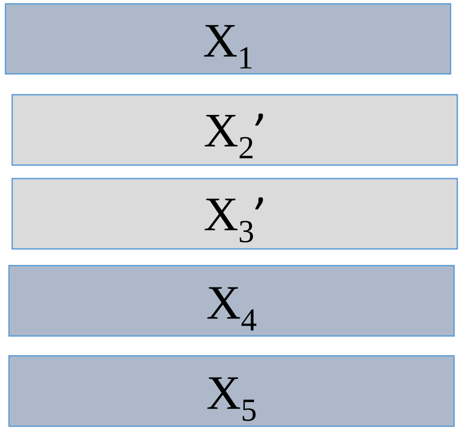
$C \le z_{ro}+2(z_{wo}+z_{rw}) \rightarrow R \le C-2(z_{wo}+z_{rw})=1$

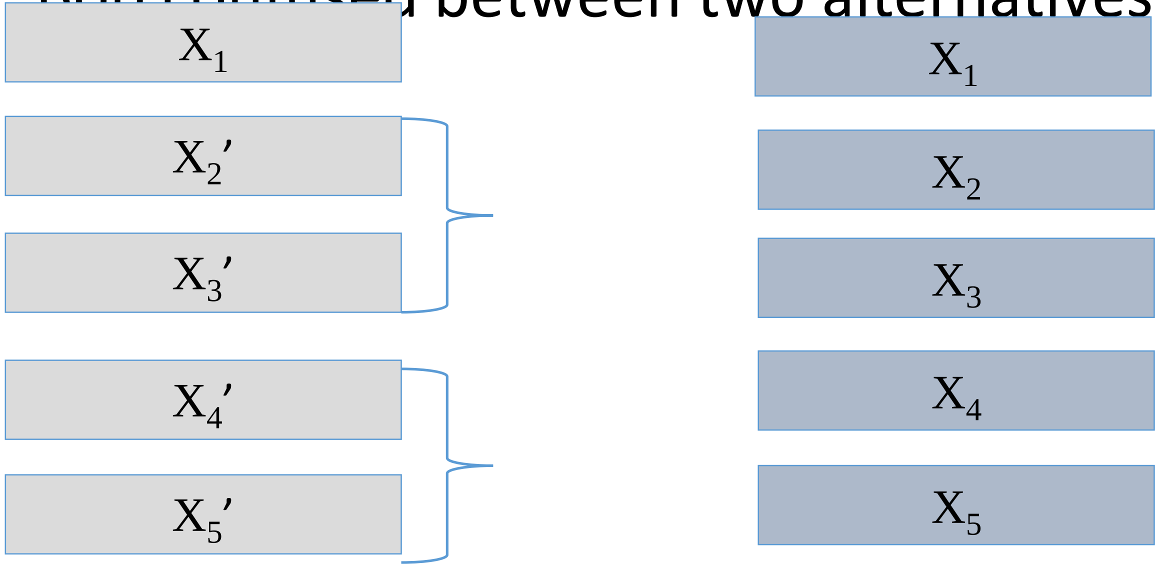


- “Stochastic” Singleton-type bound

Stochastic Singleton bound

- Calvin observes (first) Z_{ro} links
- Picks (consistent) $X'(m,r) \sim Pr(X(m,r)|x_{ro})$
  - (Not necessarily uniform)
- Picks (uniformly) one of two subsets to be z_{wo}
- Transmits symbols from $X'(m,r)$ on Z_{wo}
- TPT: Bob confused between two alternatives





Stochastic Singleton bound

- TPT: Bob confused between two alternatives

Rate too high➔Sufficiently large uncertainty in message

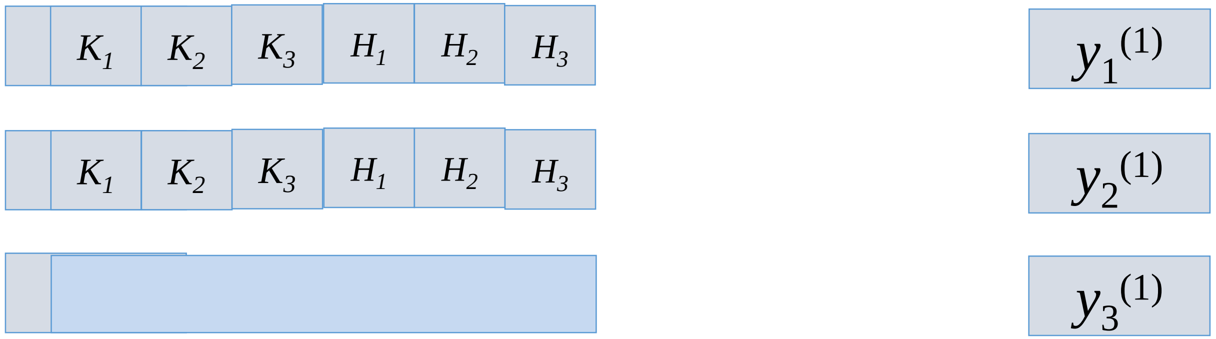
Sufficiently large uncertainty in message➔Calvin's fake message different from true message (Fano's inequality)

Bayes' theorem➔Both messages equally likely given Y observed by Bob

$\blacksquare$

Multi-round transmission with passive feedback

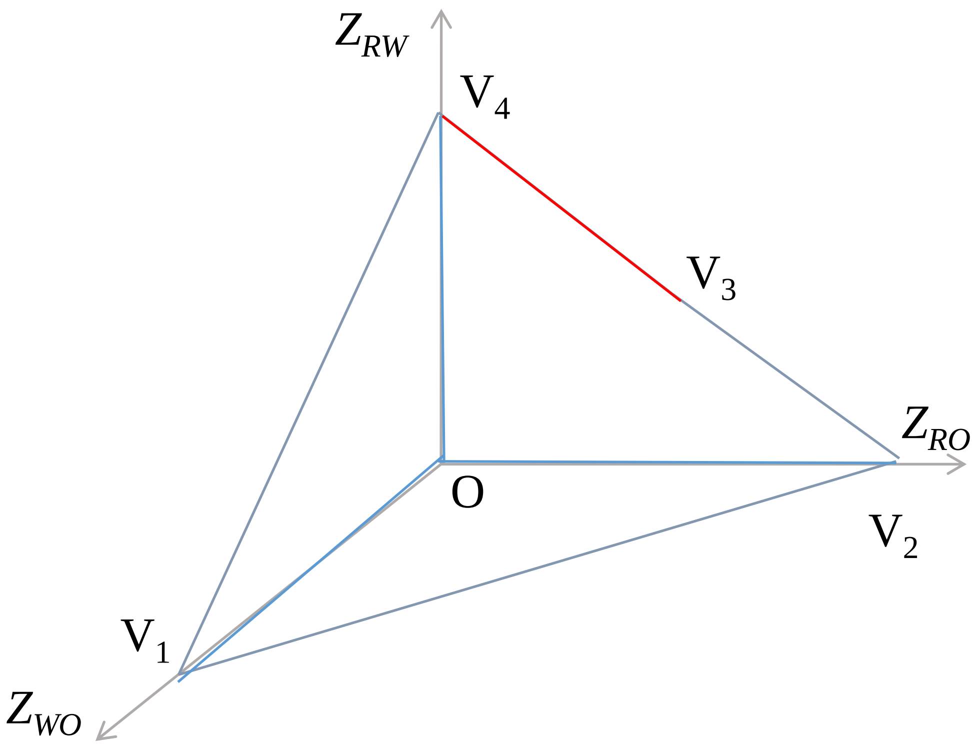
- Two-phase code (work for $Z_R <) C$
  - Phase 1: Erasure code (handle Z_W erasures)
  - Phase 2:
    - Uncorrupted links: random keys and hashes
    - Corrupted links: random vectors



Multi-round transmission with passive feedback

- *Weak adversary regime:* $R = C - Z_W$
  - Two-phase code

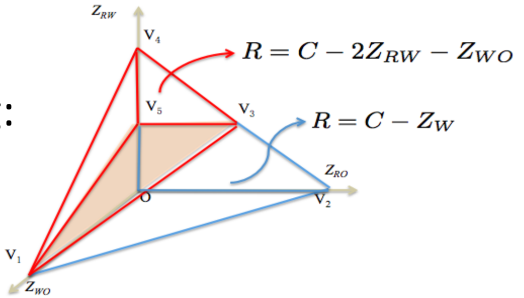
- *Strong adversary regime:*
  - Converse: *Symmetrization argument*



Summary of Results

Model		regime	reliability	reliability & secrecy
Non-causal	additive	$z_{ro} + z_{wo} + 2z_{rw} < C$	$C - (z_{rw} + z_{wo})$ $\hat{C} - (\Lambda_{z_{rw}+z_{wo}})_{max}$	$(C - z_{ro} - z_{wo} - 2z_{rw})^+$?
		$z_{ro} + z_{wo} + 2z_{rw} \geq C$	$(C - 2z_{rw} - z_{wo})^+$ $(\hat{C} - (\Lambda_{2z_{rw}+z_{wo}})_{max})^+$	0 ?
	overwrite	$z_{ro} + 2z_{wo} + 2z_{rw} < C$	$C - (z_{rw} + z_{wo})$ $\hat{C} - (\Lambda_{z_{rw}+z_{wo}})_{max}$	$(C - z_{ro} - z_{wo} - 2z_{rw})^+$?
		$z_{ro} + 2z_{wo} + 2z_{rw} \geq C$	$(C - 2z_{rw} - 2z_{wo})^+$ $(\hat{C} - (\Lambda_{2z_{rw}+2z_{wo}})_{max})^+$	0 ?
Causal w/o feedback	additive	$z_{wo} + 2z_{rw} < C$	$C - (z_{rw} + z_{wo})$ $\hat{C} - (\Lambda_{z_{rw}+z_{wo}})_{max}$	$(C - z_{ro} - z_{wo} - 2z_{rw})^+$
		$z_{wo} + 2z_{rw} \geq C$	0	0
	overwrite	$2z_{wo} + 2z_{rw} < C$	$C - (z_{rw} + z_{wo})$ $\hat{C} - (\Lambda_{z_{rw}+z_{wo}})_{max}$	$(C - z_{ro} - z_{wo} - 2z_{rw})^+$
		$z_{wo} + 2z_{rw} \geq C$	0	0
Causal with passive feedback	additive	$\{z_r = C \text{ and } 2z_w < C\} \bigcup \{z_r < C\}$	$C - (z_{rw} + z_{wo})$	$\min\{C - z_r, C - z_w\}$
		$z_r = C$ and $2z_w \geq C$	0	0
	overwrite	$z_{ro} + z_{wo} + z_{rw} < C$	$C - (z_{rw} + z_{wo})$	$(C - z_{ro} - z_{wo} - z_{rw})^+$
		$z_{ro} + z_{wo} + z_{rw} = C$	$(C - 2z_{wo} - 2z_{rw})^+$	0

Eg:

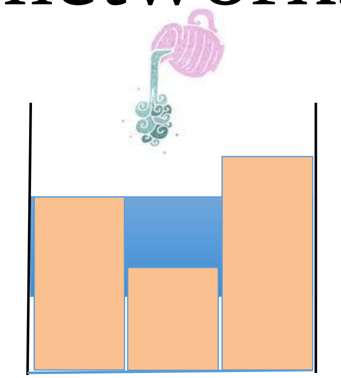


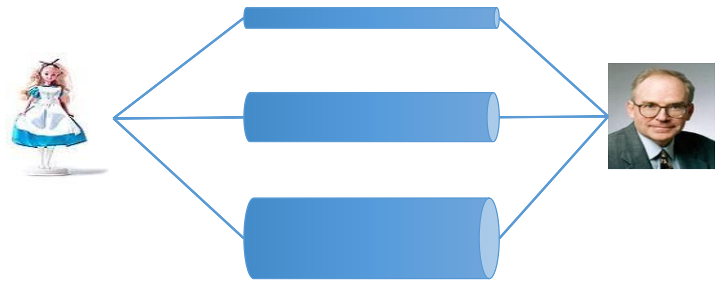
Addenda

- Information-theoretically optimal
- Reliability and Secrecy
  - $I(M; X_{Z_R}) = 0$
  - Message rate decreases by Z_R

- Computationally Efficient
  - Encoding and decoding: $\tilde{O}(C^2 n)$

- Unequal link capacity networks
  - Waterfilling



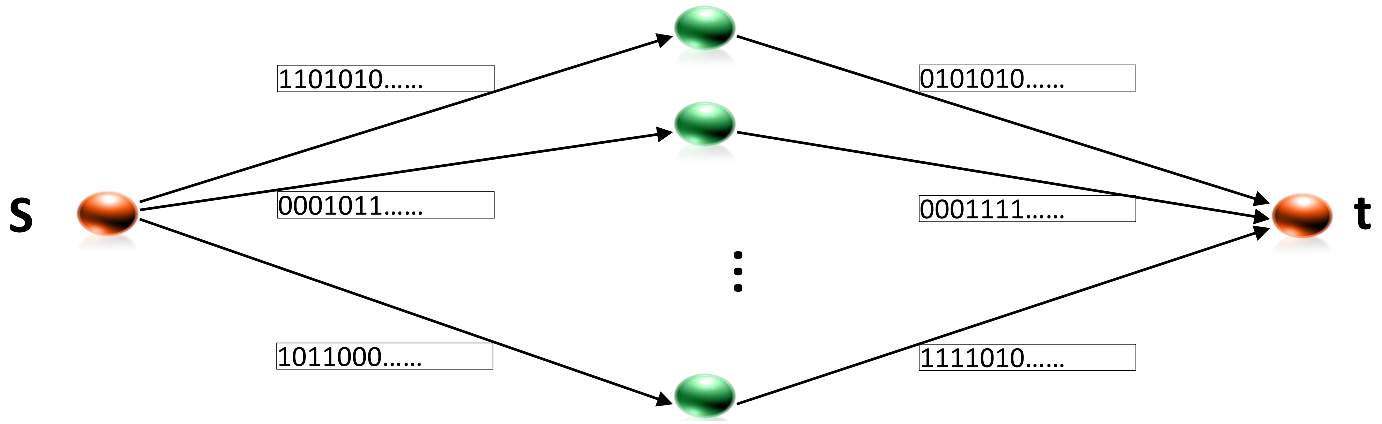


Unknown knowns part II:
End-to-End Error-Correcting Codes on Networks with **Worst-Case Symbol Errors**

Qiwen Wang

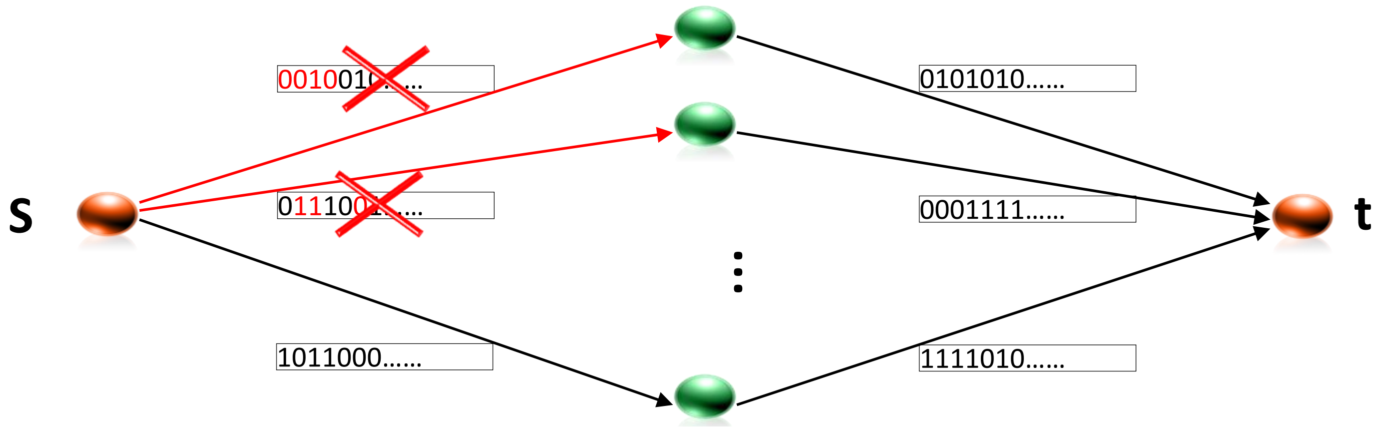
Sidharth Jaggi

Networks with Noise



	Noiseless
Throughput	[ACLY00]
Comp. efficient	[LYC03], [KM03]
Distributed	[HKMKE03]

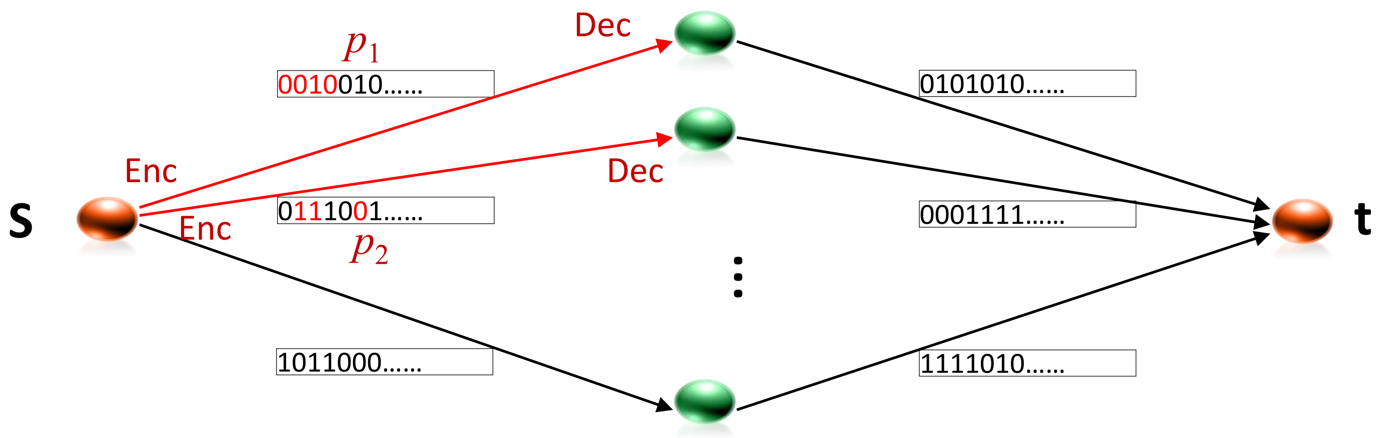
Networks with Noise



	Noiseless
Throughput	[ACLY00]
Comp. efficient	[LYC03], [KM03]
Distributed	[HKMKE03]

[YC06] R. W. Yeung, and N. Cai. Network error correction, part I: basic concepts and upper bounds. *Communications in Information and Systems*, 6(1): 19–36, 2006.
[YYZ08] S. Yang, R. W. Yeung, and Z. Zhang. Weight properties of network codes. *European Transactions on Telecommunications*, *19*(4), 371-383, 2008.
[SKK08] D. Silva, F. R. Kschischang, and R. Kötter. A rank-metric approach to error control in random network coding. *IEEE Transactions on Information Theory*, 54(9):3951–3967, 2008.
[SK09] D. Silva and F. R. Kschischang. On metrics for error correction in network coding. *IEEE Transactions on Information Theory*, 55(12):5479–5490, 2009.
[SKK10] D. Silva, F. R. Kschischang, and R. Kötter. Communication over finite-field matrix channels. *IEEE Transactions on Information Theory*, *56*(3), 1296-1305, 2010.

Networks with Noise

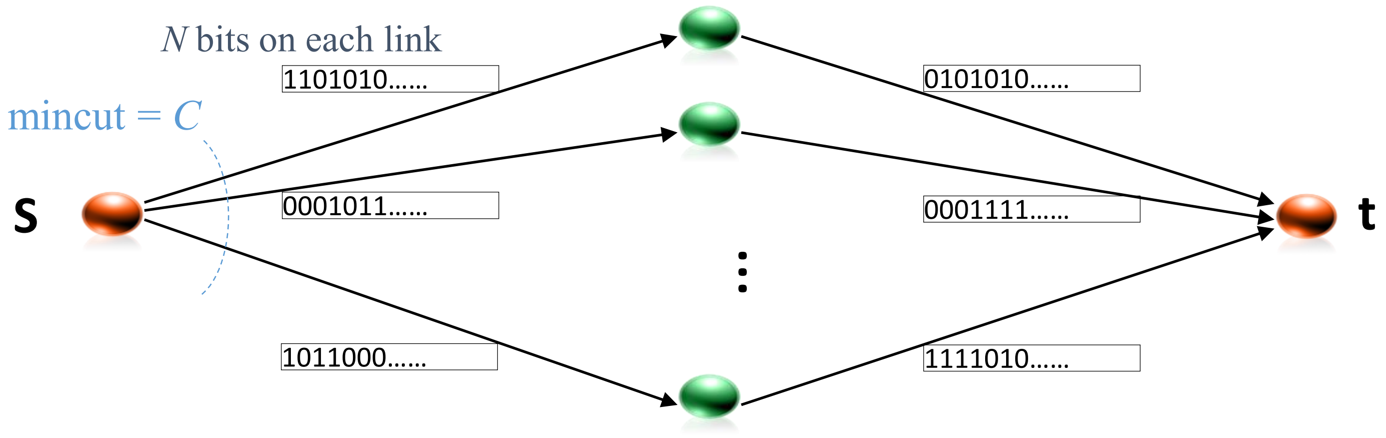


	Noiseless	Noisy	
		Packet error	
		Ran	Arb
Throughput	[ACLY00]		[YC06], [YYZ08]
Comp. efficient	[LYC03], [KM03]	[SKK10]	[SKK08], [SK09]
Distributed	[HKMKE03]		

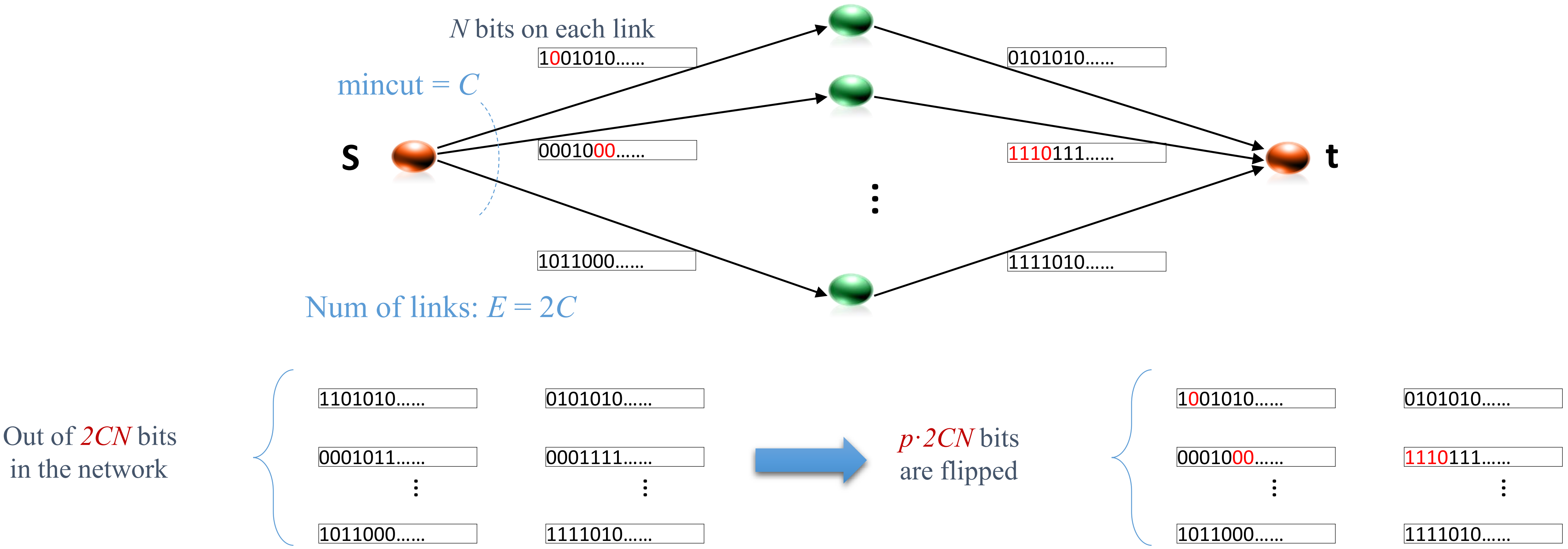
[B02] S. P. Borade, Network information flow: Limits and achievability. In *Proc. of IEEE International Symposium on Information Theory*, Lausanne, Switzerland, June 2002.

[SYC06] L. Song, R. W. Yeung, and N. Cai. A separation theorem for single-source network coding. *IEEE Transactions on Information Theory*, 52(5):1861–1871, 2006.

Worst-case Noise： Example

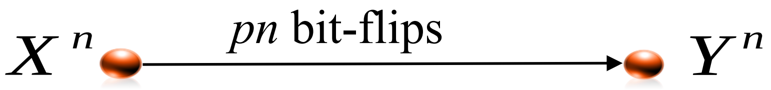


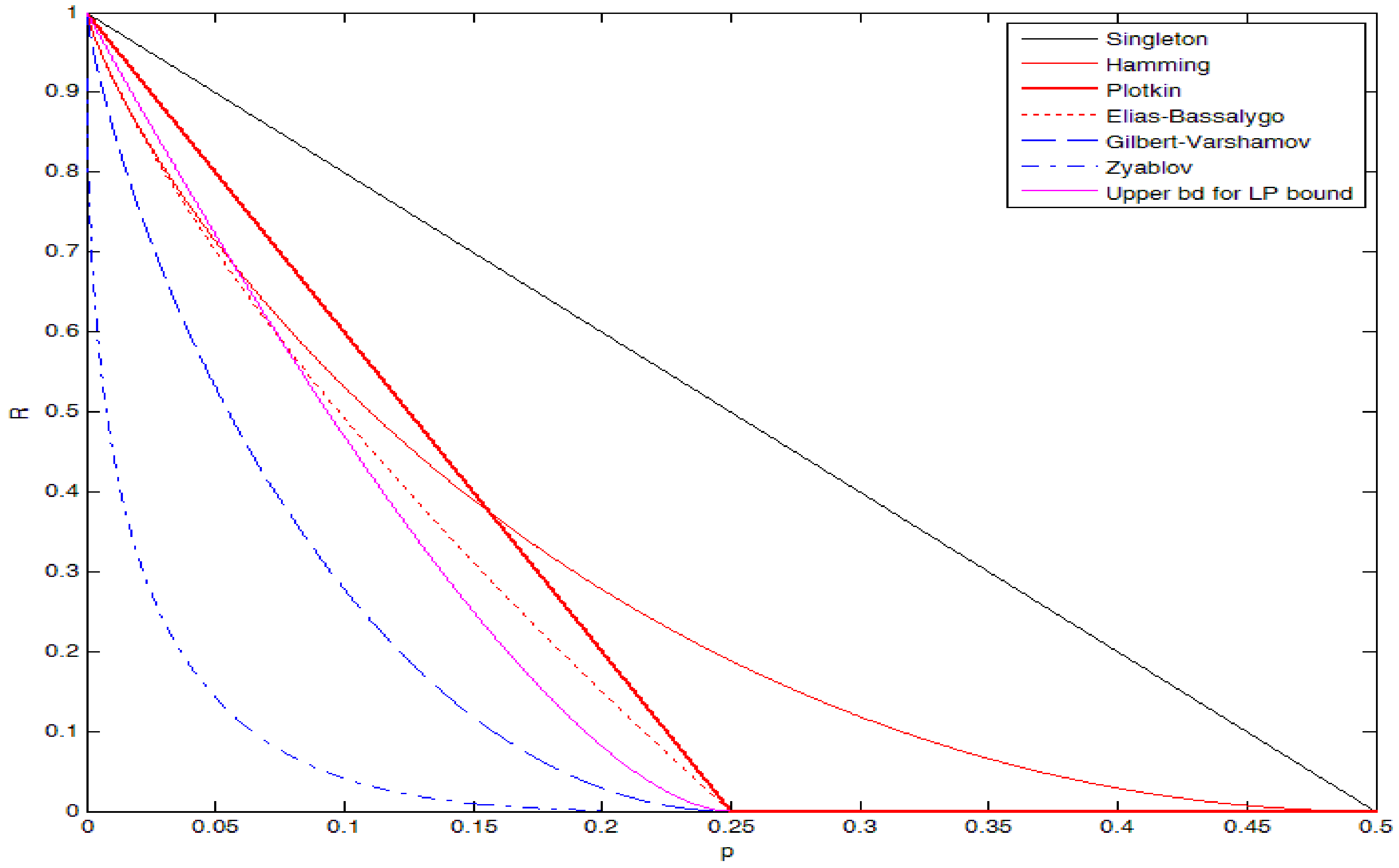
Worst-case Noise: Example



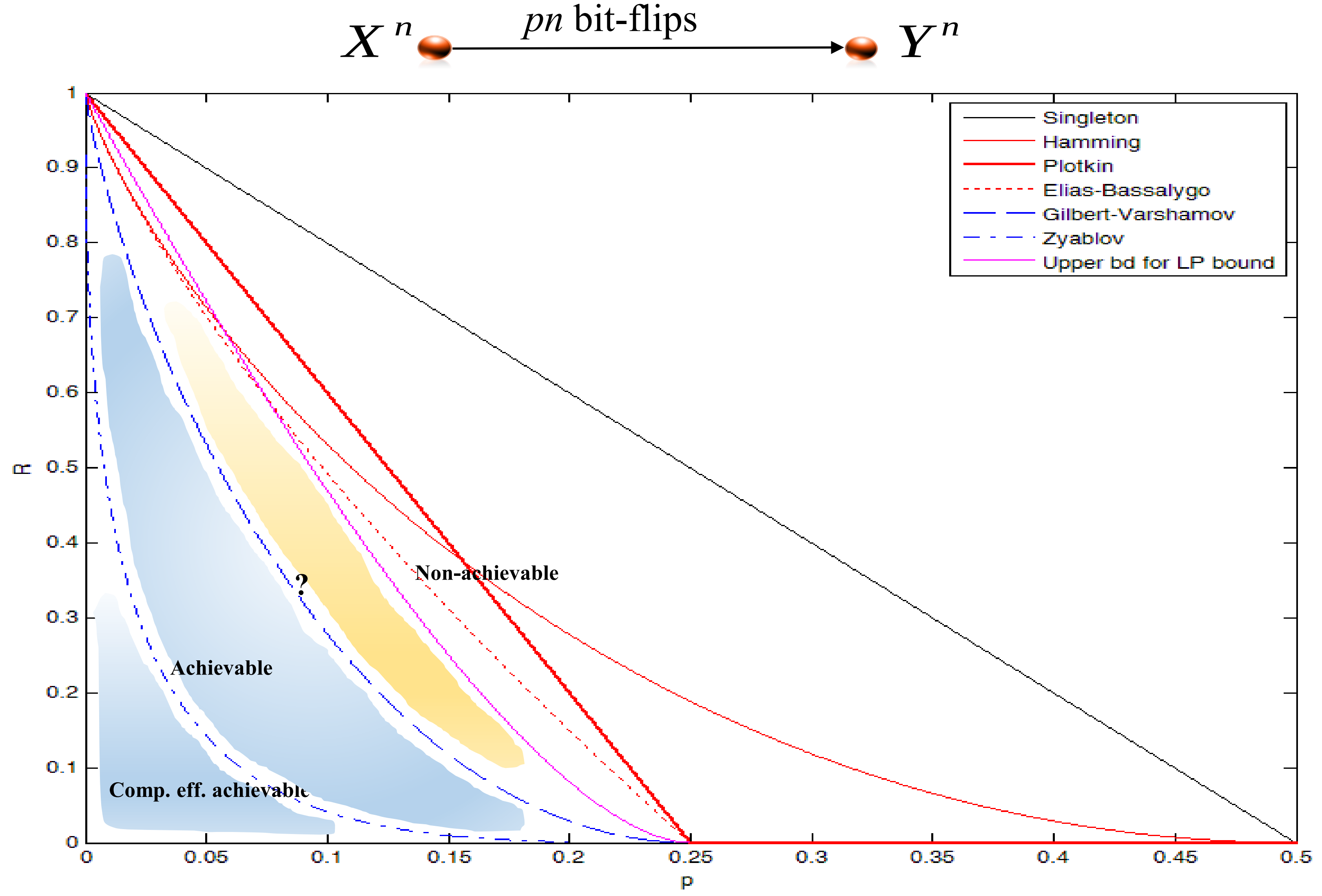
What is the rate region and achievable schemes for this noisy network (normalized by CN)

Revisit: Point-to-Point Communication

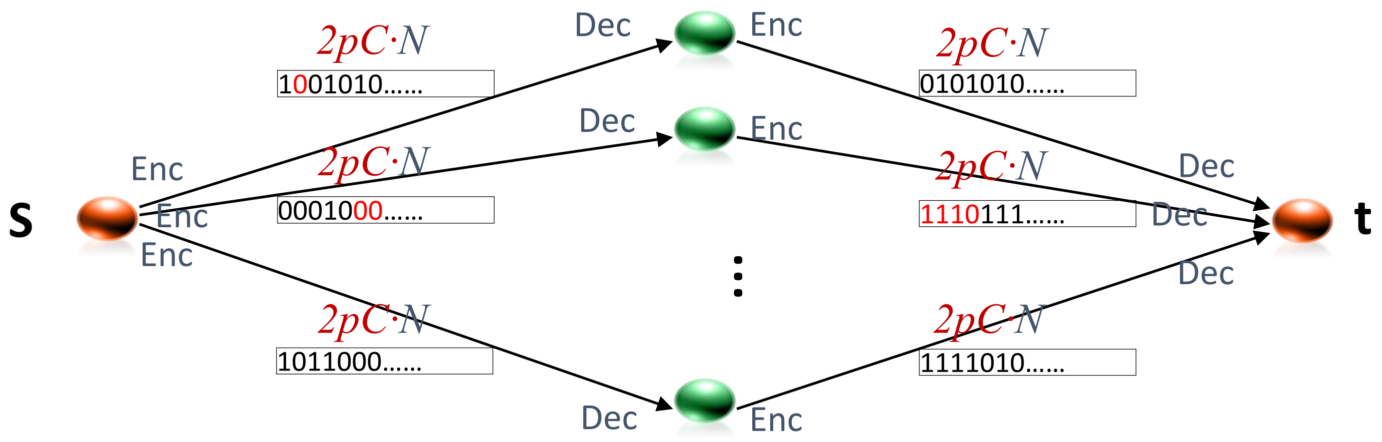




Revisit: Point-to-Point Communication



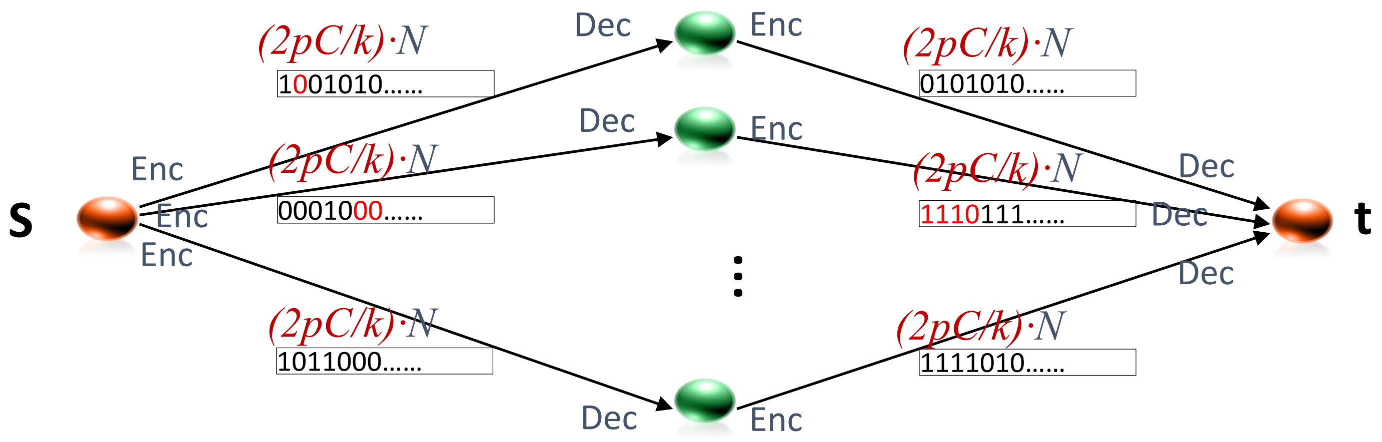
Benchmark 1



Link-by-link error-correcting codes (Gilbert-Varshamov construction)

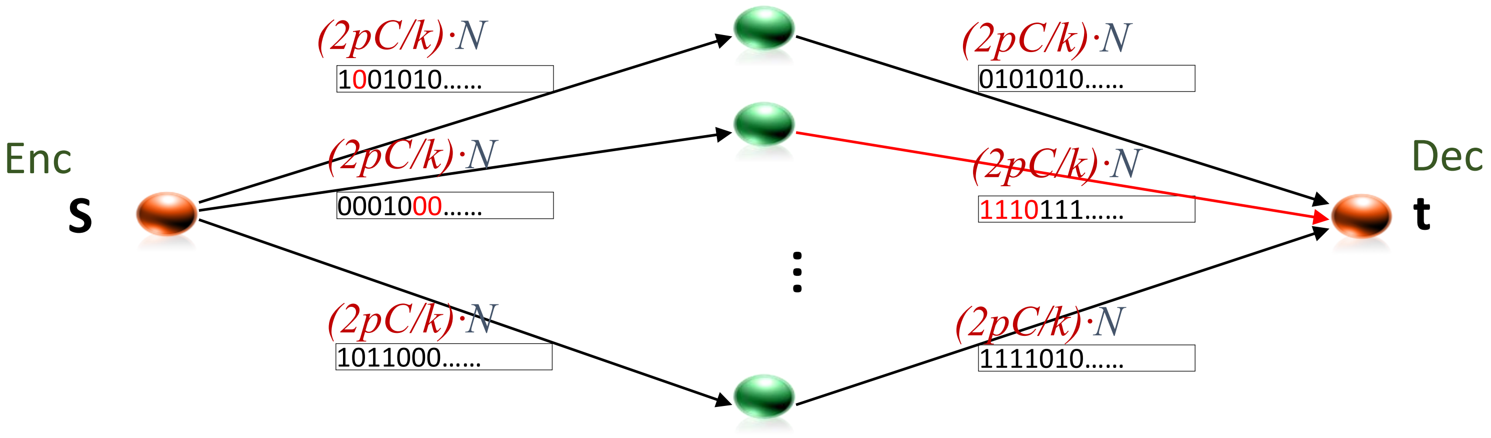
$$R = 1 - H(4Cp)$$

Benchmark 2



$$R_{link} = 1 - H\left(\frac{4Cp}{k}\right)$$

Benchmark 2

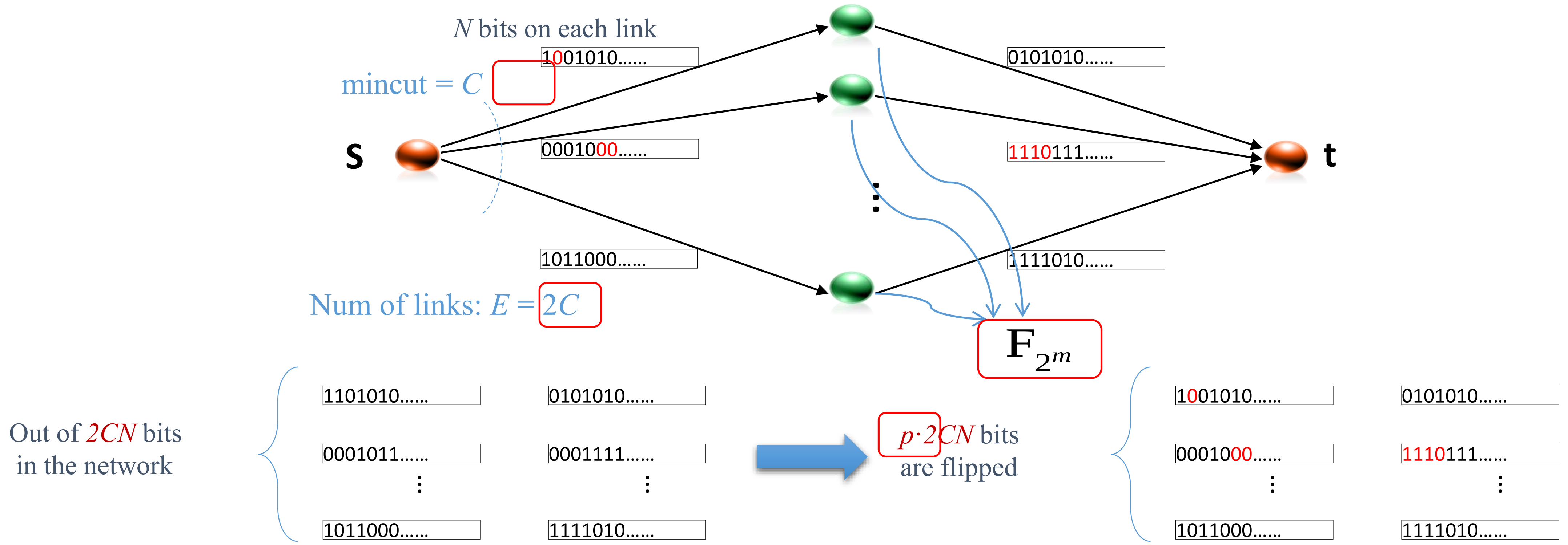


$$R_{link} = 1 - H\left(\frac{4Cp}{k}\right)$$

At most k links corrupted,

$$R = \left(1 - \frac{2k}{C}\right) \cdot R_{link} = \left(1 - \frac{2k}{C}\right) \cdot \left(1 - H\left(\frac{4Cp}{k}\right)\right)$$

Worst-case Noise: Example



What is the rate region and achievable schemes for this noisy network (normalized by CN)

Main Results

Achievable schemes:

Gilbert-Varshamov

- *Coherent* GV-type codes achieve rates at least

$$1-\frac{E}{C}H(2p)$$

- *Non-coherent* GV-type codes achieve rates at least

$$1-\frac{E}{C}H(2p)$$

$2^{O(n)}$

Zyablov

- Concatenated network codes achieve rates at least

$$\max_{0<r<1-\frac{E}{C}H(2p)} r\cdot\left(1-\frac{2p}{H^{-1}(\frac{C}{E}(1-r))}\right)$$

$n^{O(1)}$

Converses:

Hamming

- For all $p<\frac{C}{2Em}$

$$R\leq 1-\frac{E}{C}H(p)$$

Plotkin

- For all $p<\frac{C}{E}(1-\frac{C}{E})$

$$R\leq 1-\frac{E^2}{CE-C^2}p$$

- If $p\geq\frac{C}{E}(1-\frac{C}{E})$

$$R=0$$

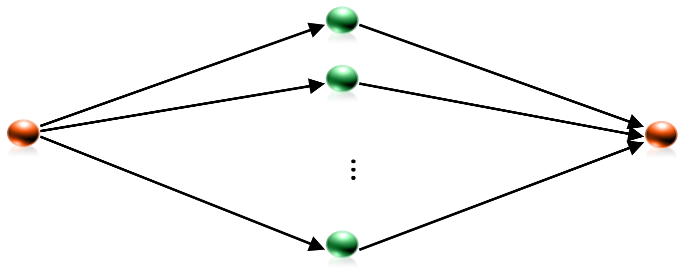
Elias-Bassalygo

- For all $p<\frac{C}{2Em}(1-\frac{C}{2Em})$

$$R<1-\frac{E}{C}H\left(\frac{1-\sqrt{1-4p}}{2}\right)$$

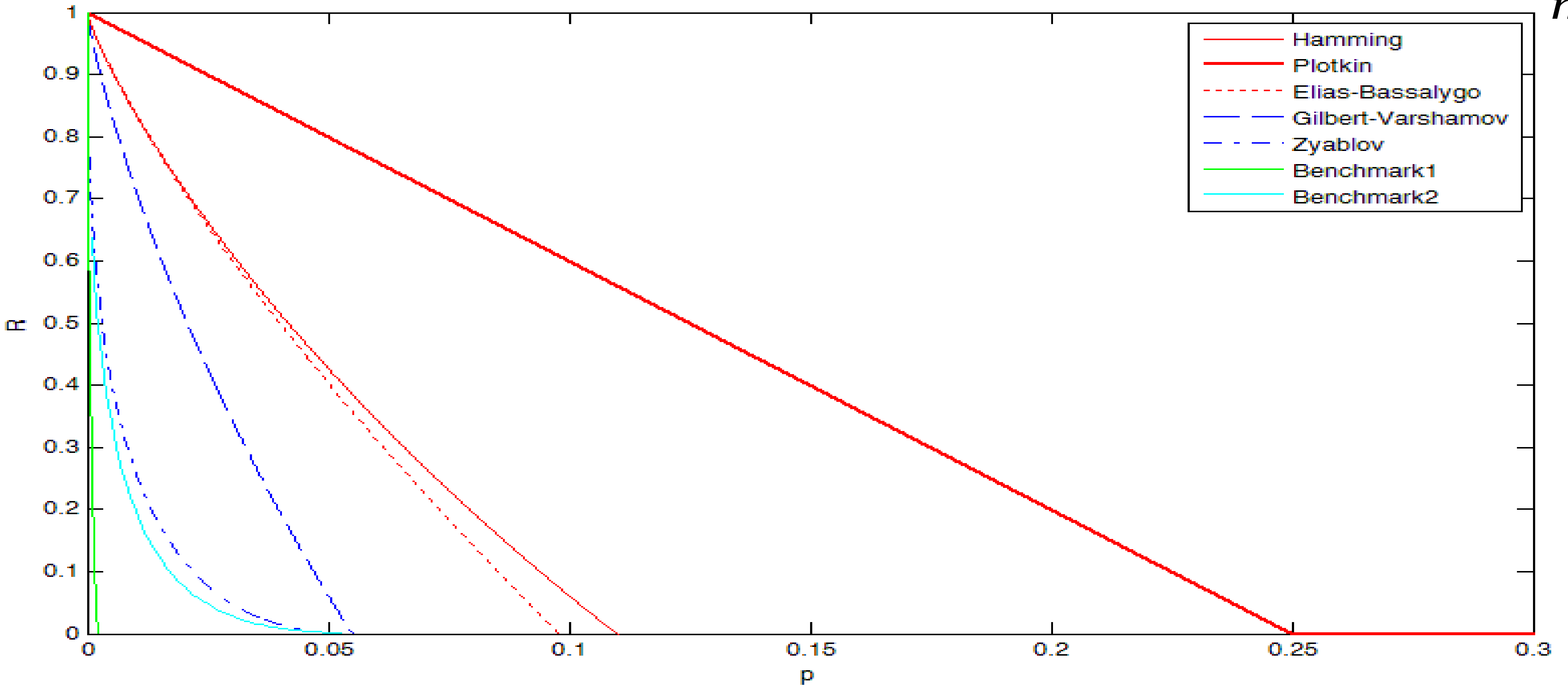
- *Coherent*: the internal coding coefficients are *known* in advance
- *Non-coherent*: the internal coding coefficients are *unknown* in advance

Main Results

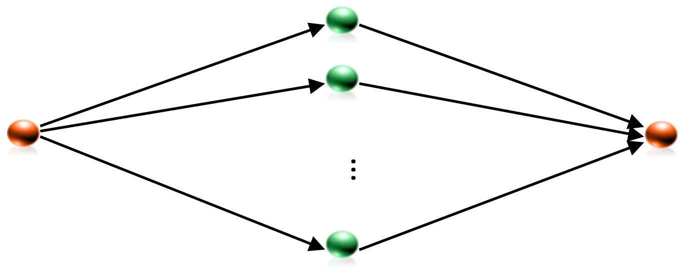


$E = 100, C = 50$

$m = 2$

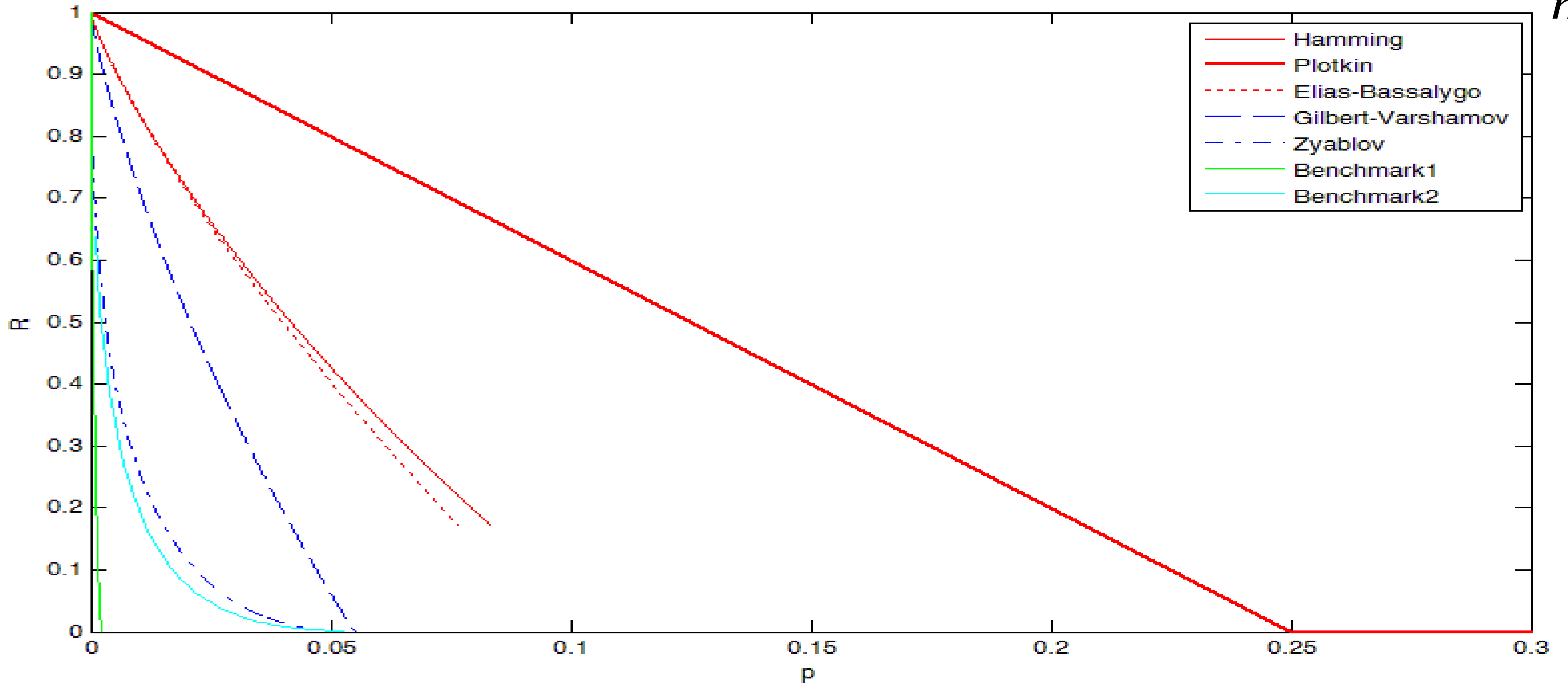


Main Results



$E = 100, C = 50$

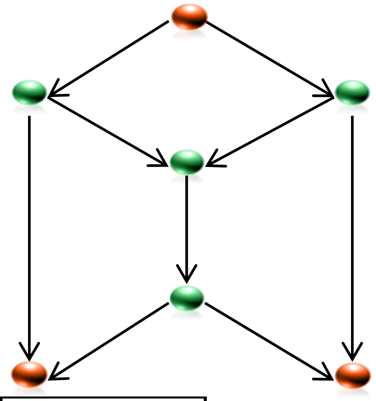
$m = 3$

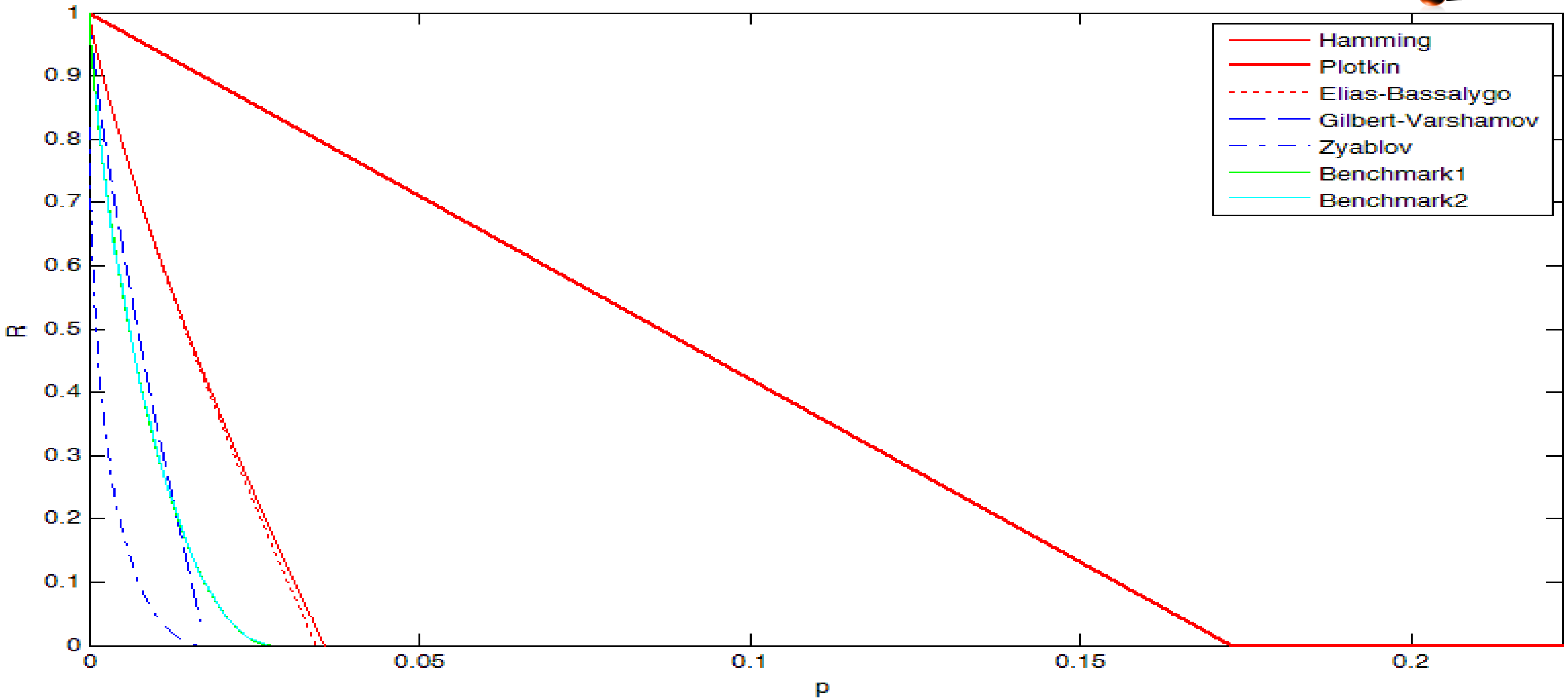


Main Results

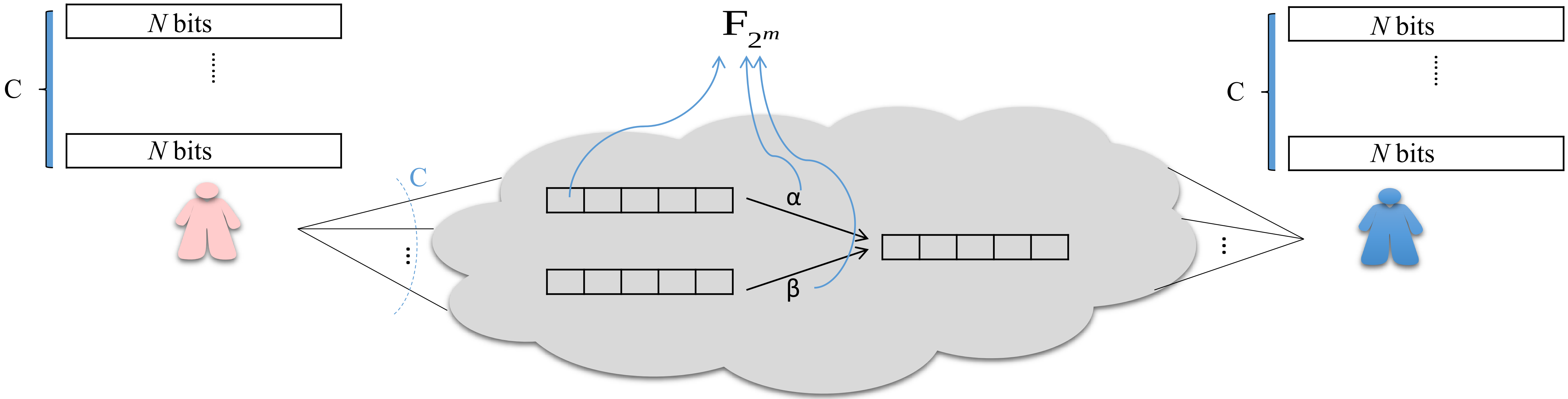
$E = 9, C = 2$

$m = 2$

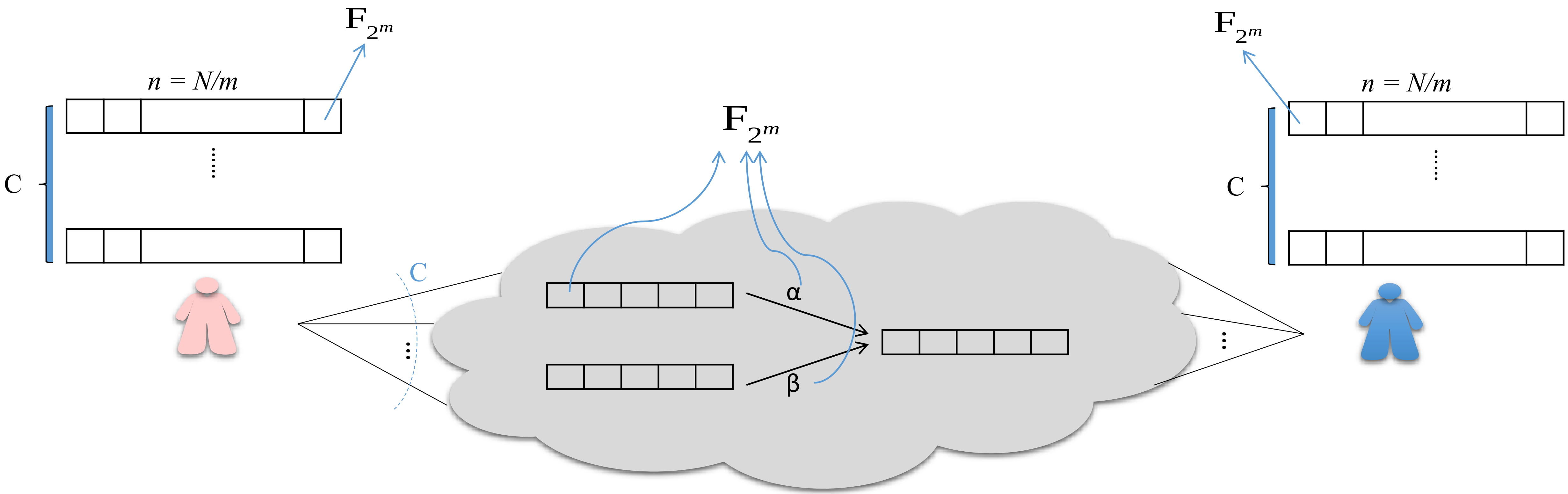




Model



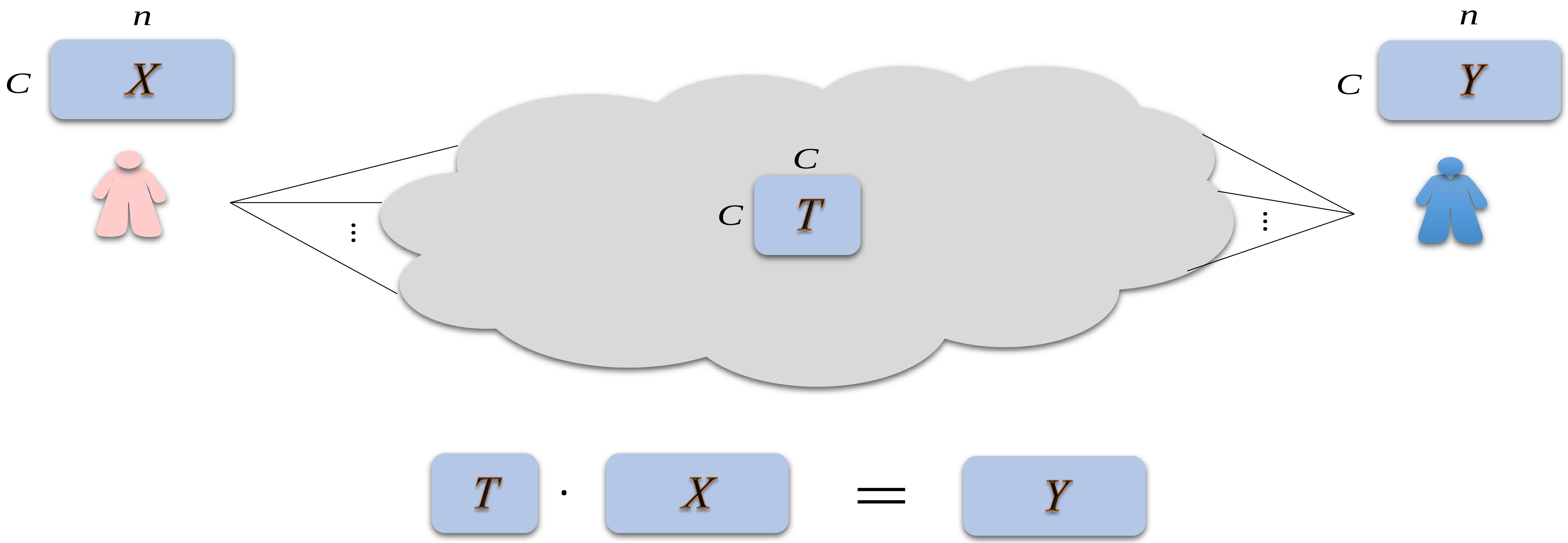
Model



[KM03] R. Kötter and M. Médard. An algebraic approach to network coding. *IEEE/ACM Transactions on Networking, 2003*.

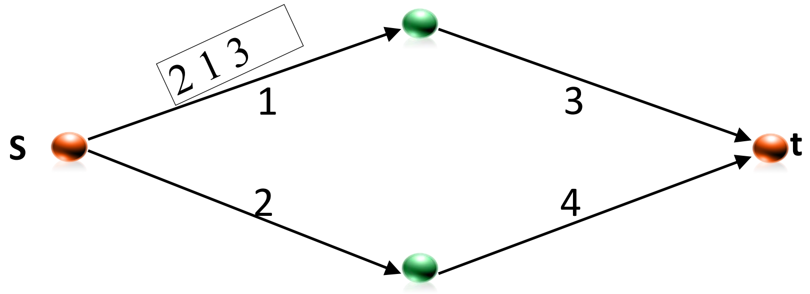
[HKMKM03] T. Ho, R. Köetter, M. Médard, D. R. Karger, and M. Effros. The benefits of coding over routing in a randomized setting. In *Proc. of IEEE International Symposium on Information Theory*, Yokohama, Japan, June 2003.

Model



Finite field $\mathbf{F}_{2^m}$ to binary field $\mathbf{F}_2$

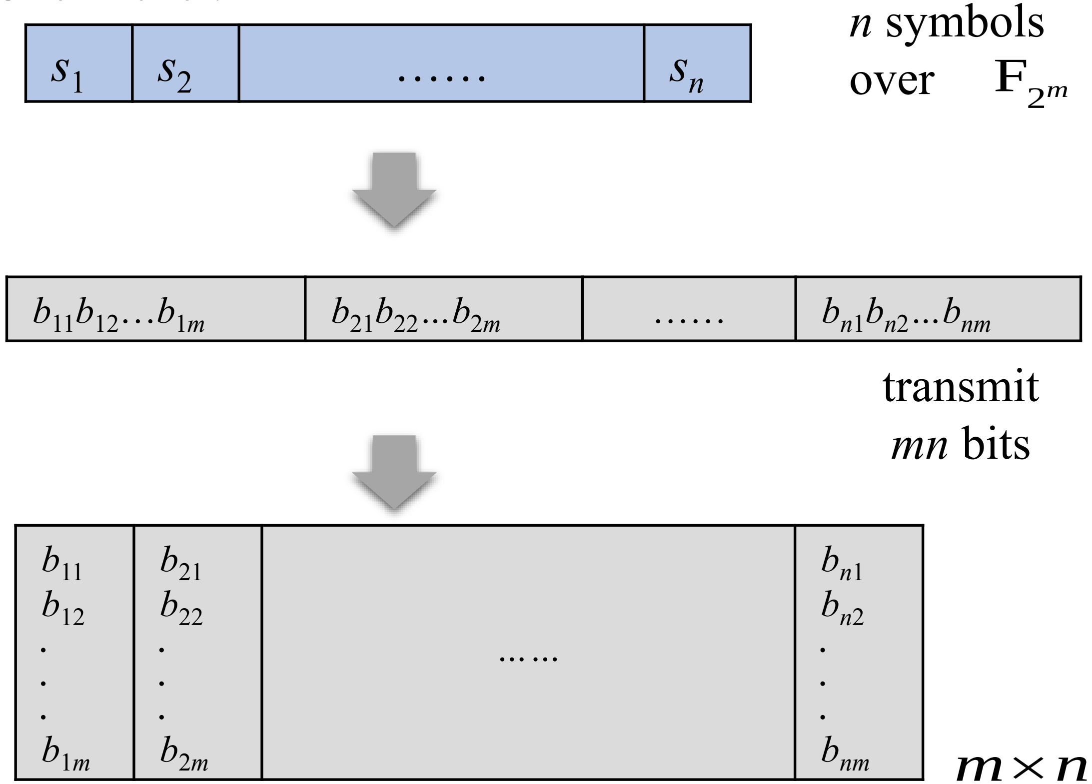
Example:



$$X_1 = \begin{pmatrix} 2 & 1 & 3 \end{pmatrix}_{\mathbf{F}_4}$$

$$\begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \end{pmatrix}_{\mathbf{F}_2}$$

One Packet:



n symbols over $\mathbf{F}_{2^m}$

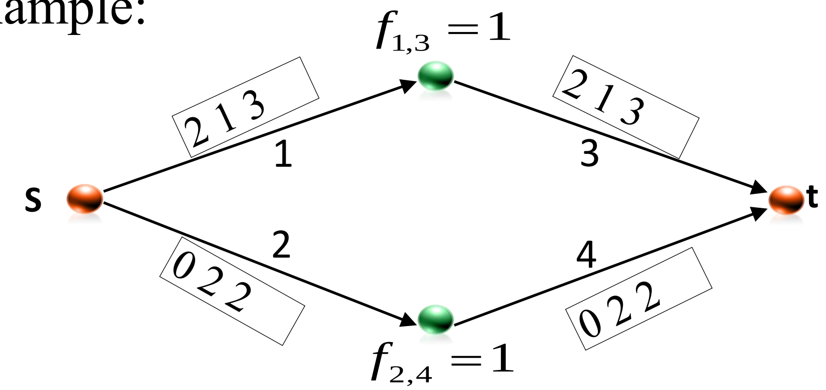
transmit mn bits

$m \times n$ binary matrix

[JEHM04] S. Jaggi, M. Effros, T. Ho, and M. Médard. On linear network coding. In *Proceedings of 42nd Annual Allerton Conference on Communication, Control, and Computing*, Monticello, IL, 2004.

Finite field $\mathbf{F}_{2^m}$ to binary field $\mathbf{F}_2$

Example:



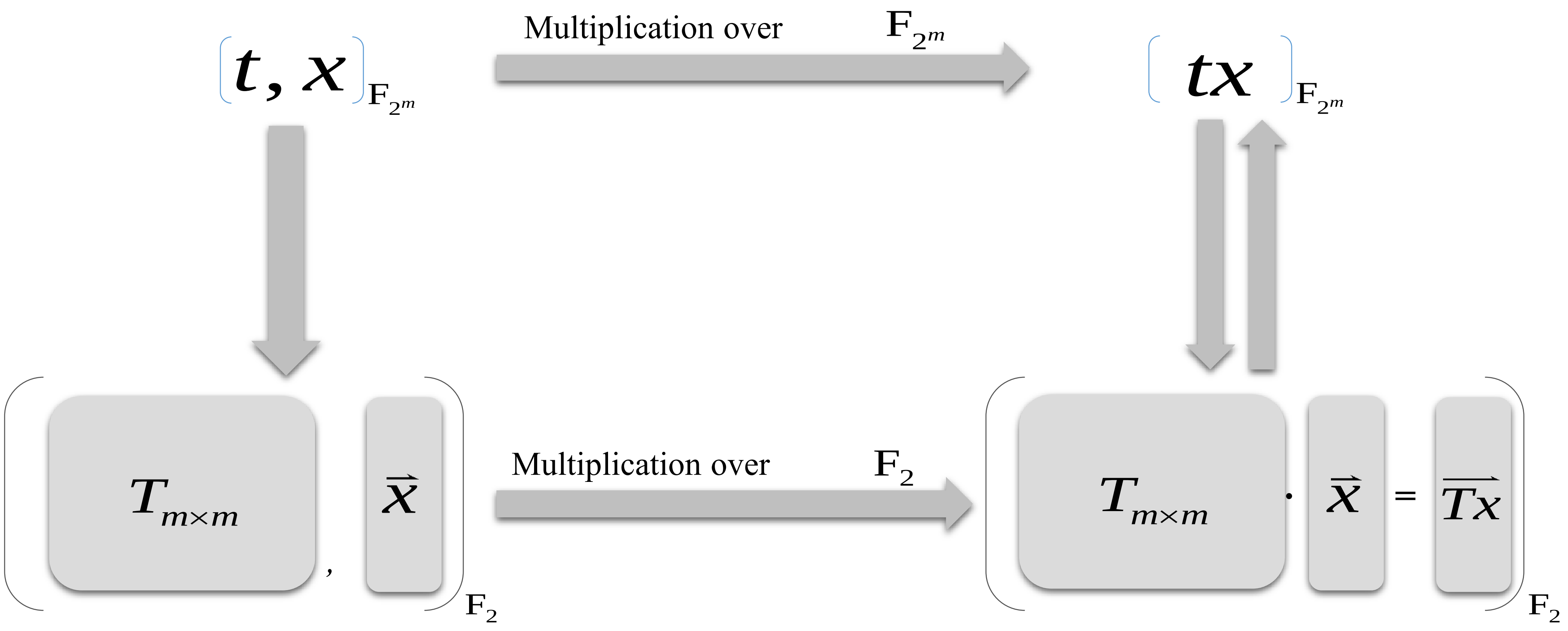
$$X = \begin{pmatrix} 2 & 1 & 3 \\ \hdashline 0 & 2 & 2 \end{pmatrix} \qquad T = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

$$Y = TX = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}_{\mathbf{F}_4} \cdot \begin{pmatrix} 2 & 1 & 3 \\ \hdashline 0 & 2 & 2 \end{pmatrix}_{\mathbf{F}_4} = \begin{pmatrix} 2 & 1 & 3 \\ \hdashline 0 & 2 & 2 \end{pmatrix}_{\mathbf{F}_4}$$

$$Y = TX = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}_{\mathbf{F}_2} \cdot \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \\ \hdashline 0 & 1 & 1 \\ 0 & 0 & 0 \end{pmatrix}_{\mathbf{F}_2} = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \\ \hdashline 0 & 1 & 1 \\ 0 & 0 & 0 \end{pmatrix}_{\mathbf{F}_2}$$

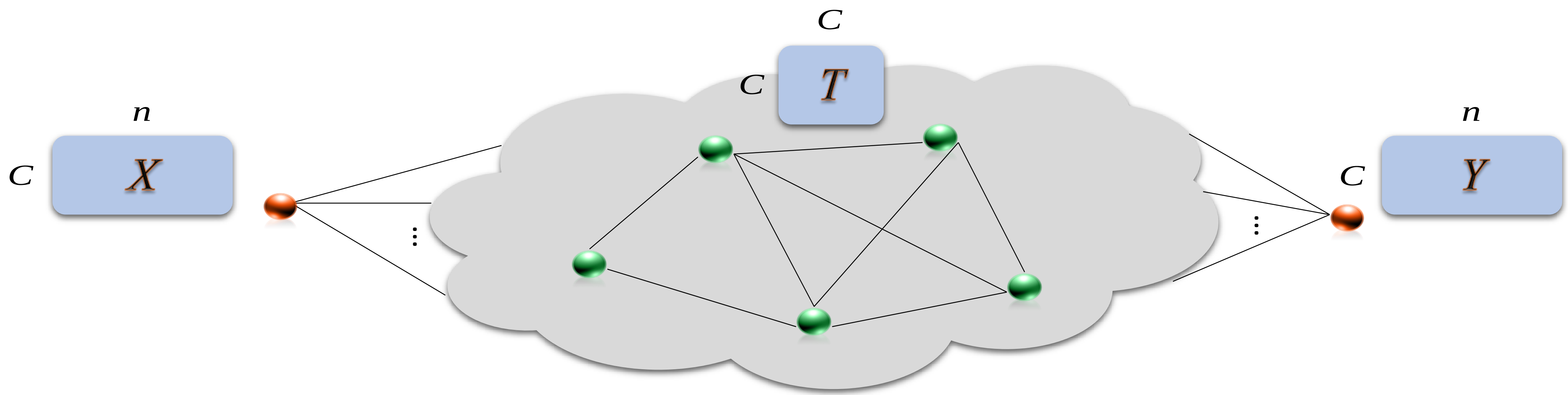
[JEHM04] S. Jaggi, M. Effros, T. Ho, and M. Médard. On linear network coding. In *Proceedings of 42nd Annual Allerton Conference on Communication, Control, and Computing*, Monticello, IL, 2004.

Finite field $\mathbb{F}_{2^m}$ to binary field $\mathbb{F}_2$



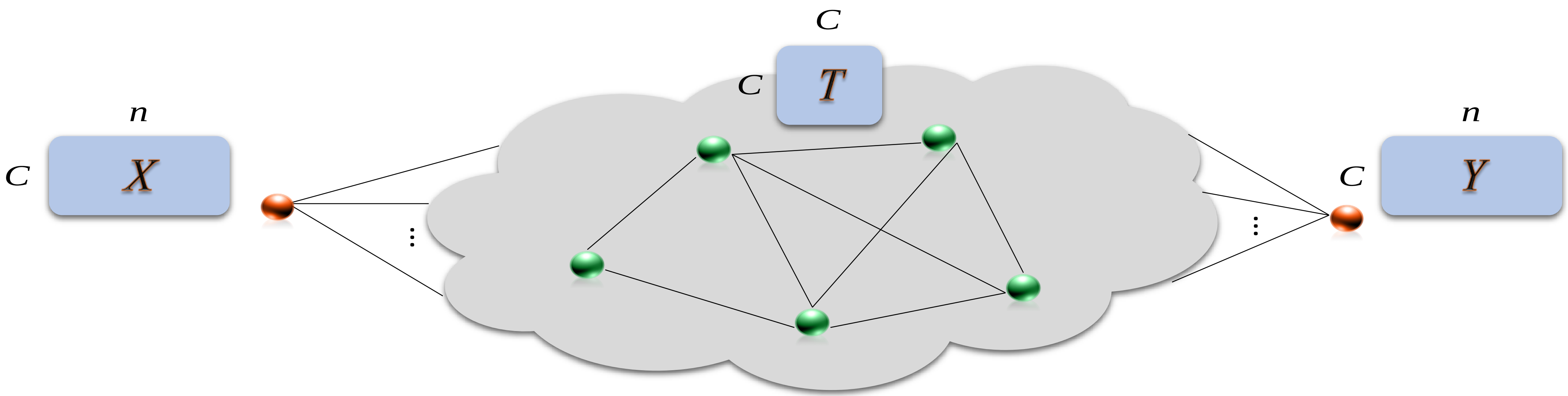
[JEHM04] S. Jaggi, M. Effros, T. Ho, and M. Médard. On linear network coding. In *Proceedings of 42nd Annual Allerton Conference on Communication, Control, and Computing*, Monticello, IL, 2004.

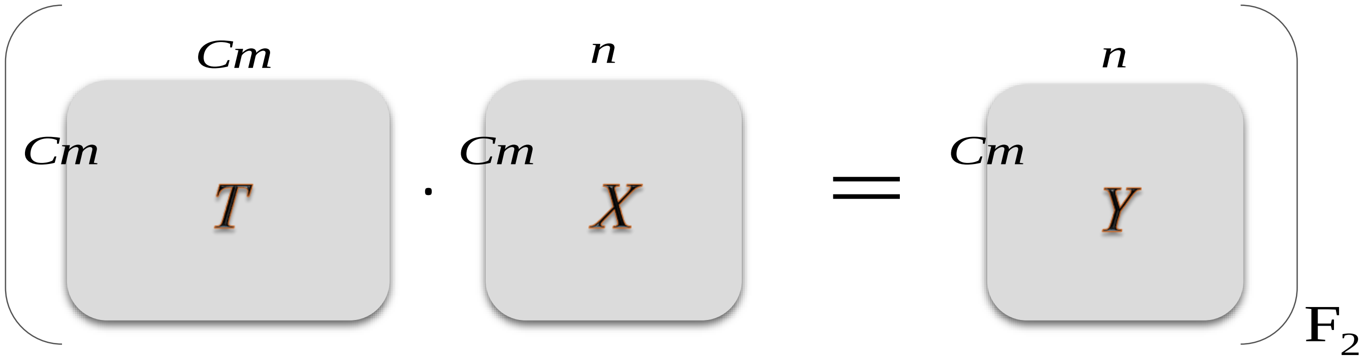
Noiseless Network



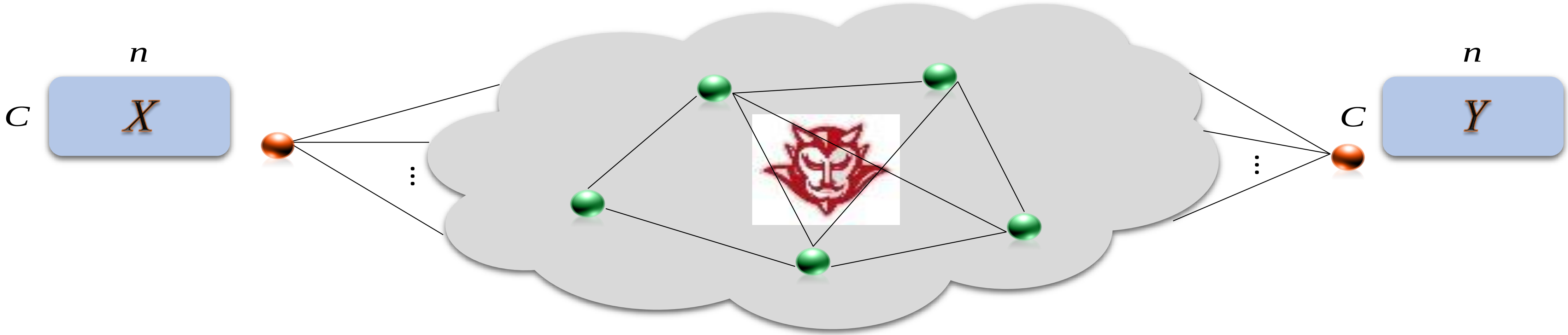
$$\left(T_{c \times c} \cdot X_{c \times n} = Y_{c \times n} \right)_{\mathbb{F}_{2^m}}$$

Noiseless Network

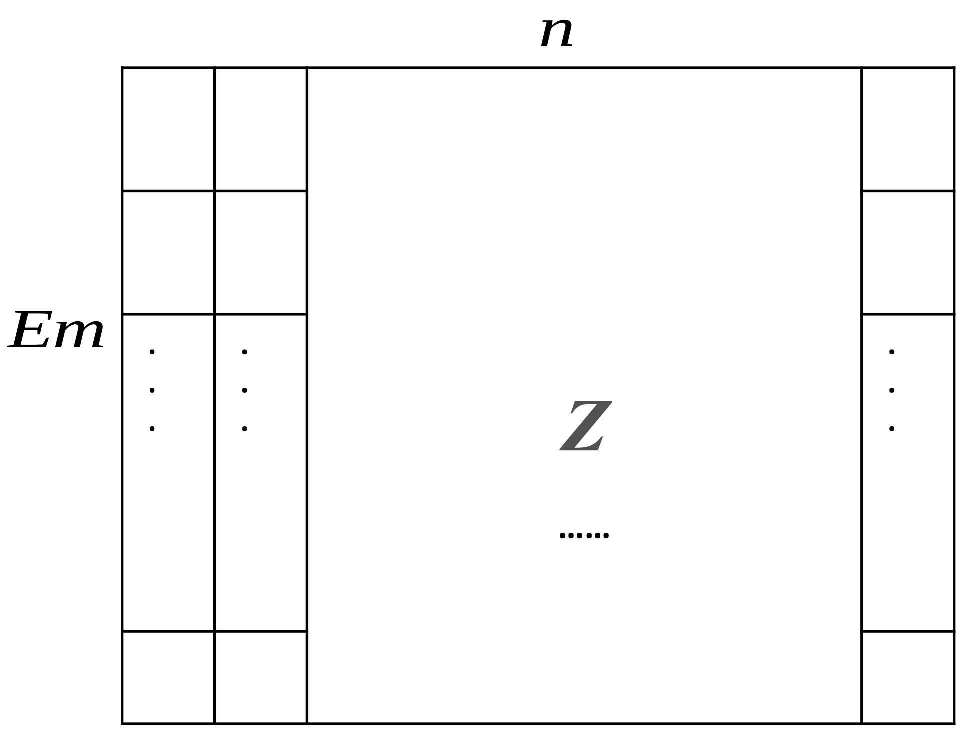




With noise

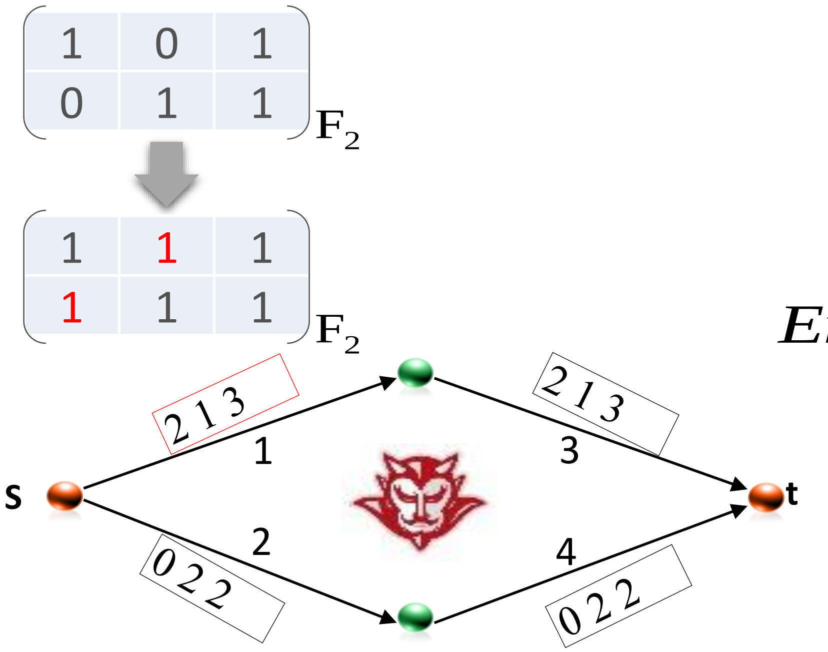


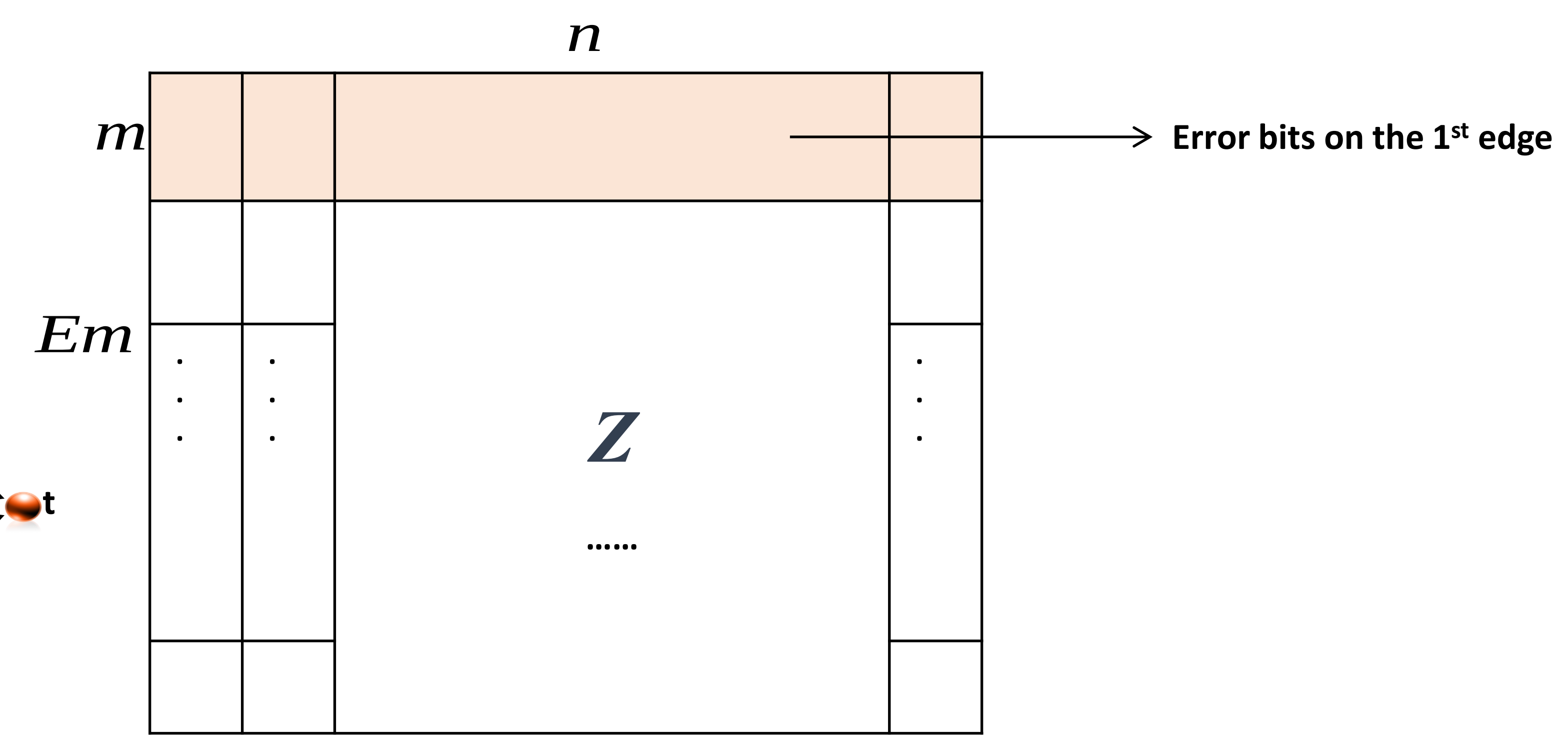
Noise Model



Worst-case bit-flip error matrix Z:
no more than *pEmn* 1s, arbitrarily distributed
***E*: num of edges in the network**

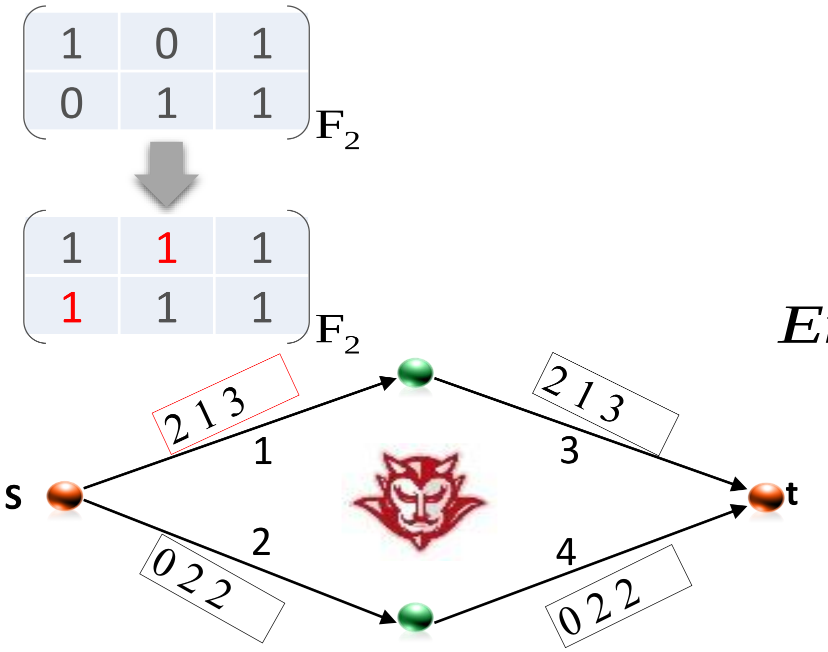
Noise Model

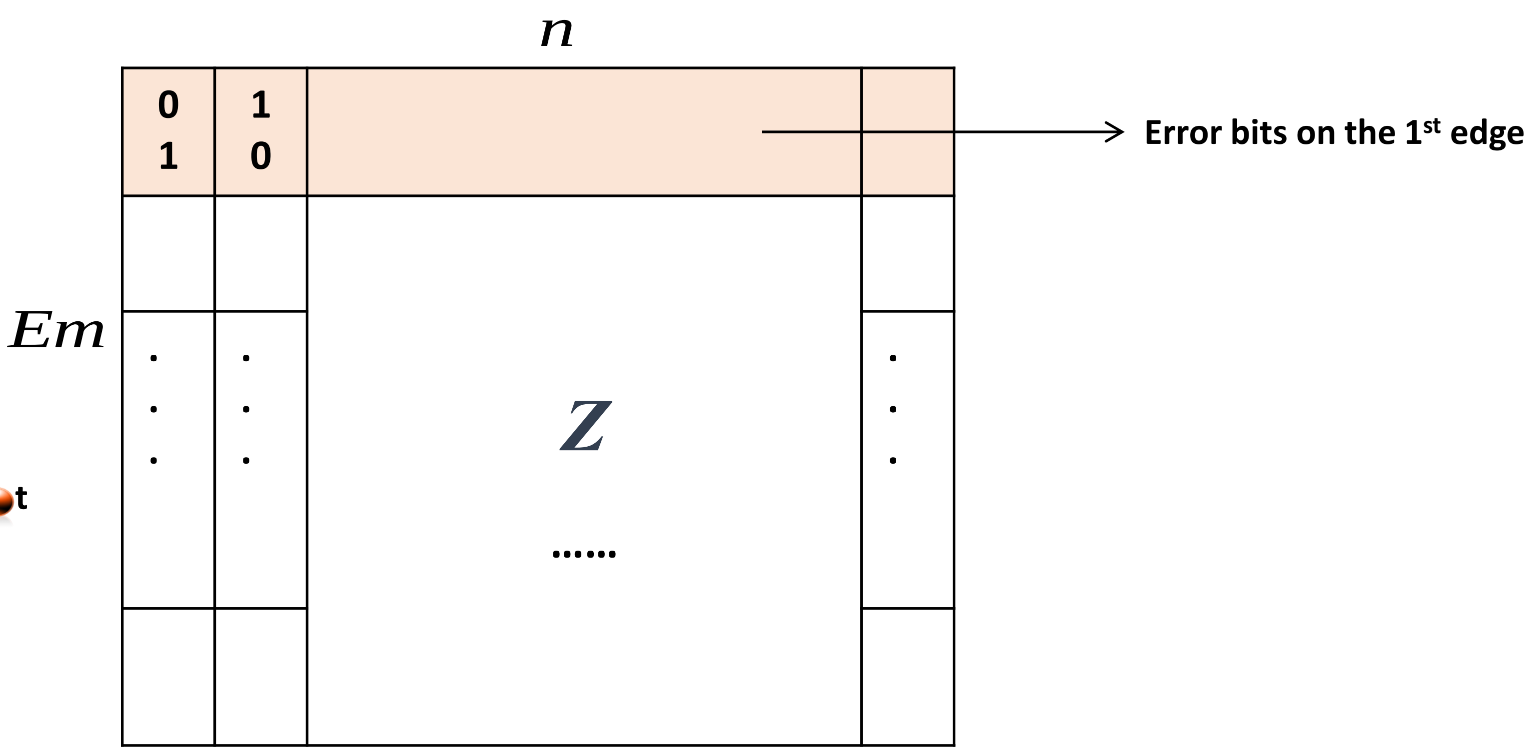




Worst-case bit-flip error matrix Z:
no more than *pEmn* 1s, arbitrarily distributed
E: num of edges in the network

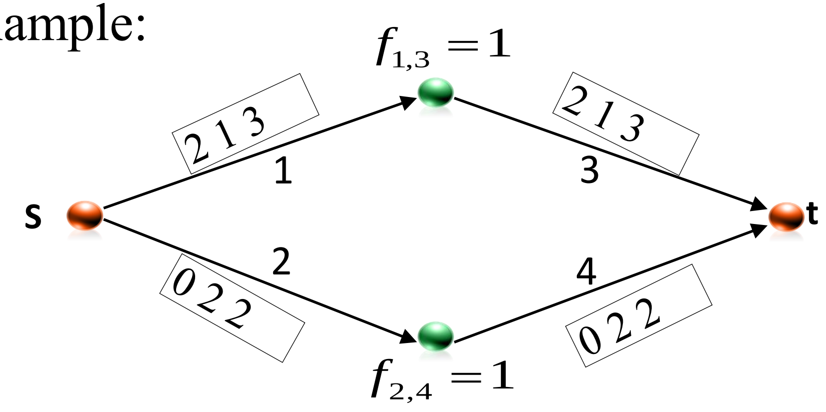
Noise Model





Worst-case bit-flip error matrix Z:
no more than *pEmn* 1s, arbitrarily distributed
E: num of edges in the network

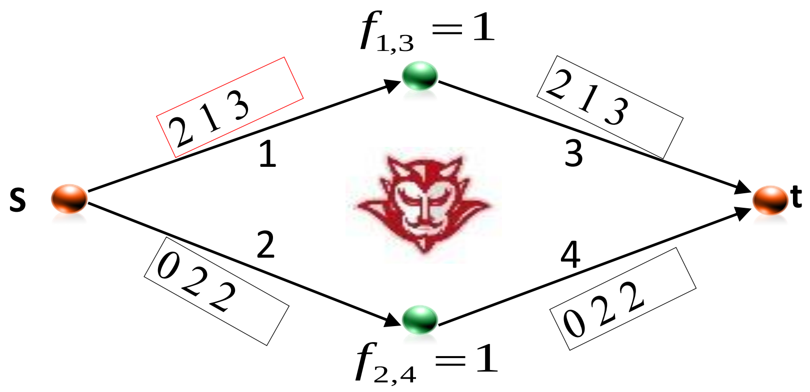
Example:



$$X=\begin{pmatrix} 2 & 1 & 3 \\ 0 & 2 & 2 \end{pmatrix} \qquad T=\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

$$Y=TX=\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}_{\mathbf{F}_4} \cdot \begin{pmatrix} 2 & 1 & 3 \\ 0 & 2 & 2 \end{pmatrix}_{\mathbf{F}_4} = \begin{pmatrix} 2 & 1 & 3 \\ 0 & 2 & 2 \end{pmatrix}_{\mathbf{F}_4}$$

$$Y=TX=\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}_{\mathbf{F}_2} \cdot \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \\ 0 & 1 & 1 \\ 0 & 0 & 0 \end{pmatrix}_{\mathbf{F}_2} = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \\ 0 & 1 & 1 \\ 0 & 0 & 0 \end{pmatrix}_{\mathbf{F}_2}$$



$$X = \begin{pmatrix} 2 & 1 & 3 \\ 0 & 2 & 2 \end{pmatrix}_{\mathbb{F}_4}$$

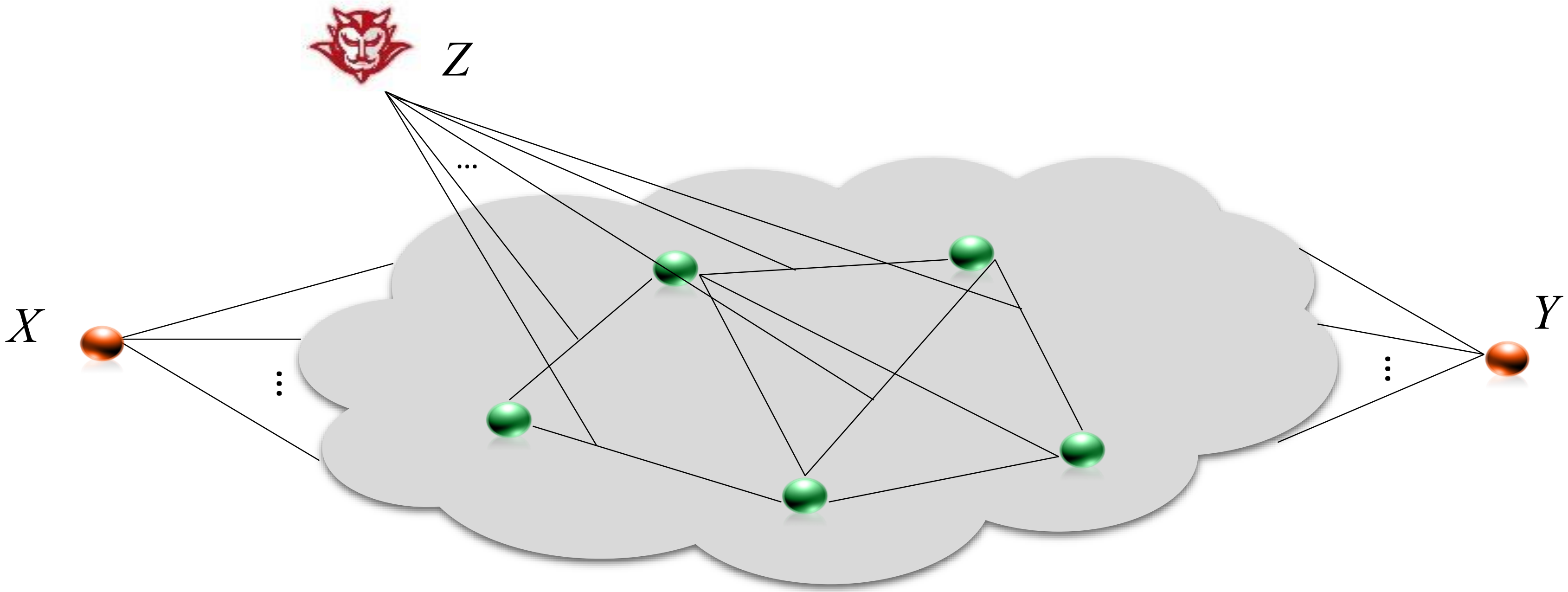
$$T = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}_{\mathbb{F}_4}$$

$$\hat{T} = \begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \end{pmatrix}_{\mathbb{F}_4}$$

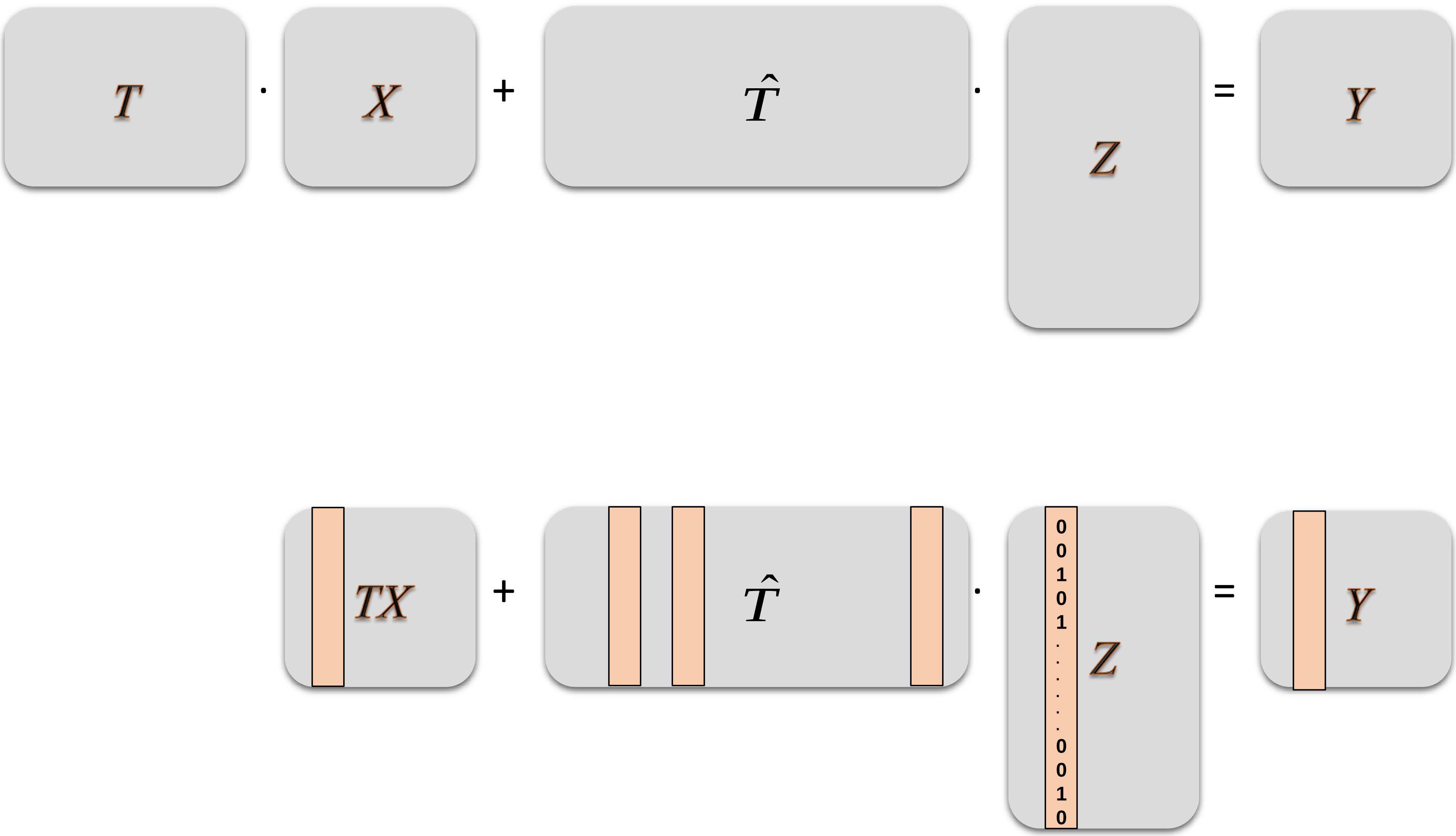
$$Y = TX + Z\hat{T} \quad \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}_{\mathbb{F}_2} \cdot \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \\ 0 & 1 & 1 \\ 0 & 0 & 0 \end{pmatrix}_{\mathbb{F}_2} + \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 \end{pmatrix}_{\mathbb{F}_2} \cdot \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}_{\mathbb{F}_2}$$

$$= \begin{pmatrix} 1 & 1 & 1 \\ 1 & 1 & 1 \\ 0 & 1 & 1 \\ 0 & 0 & 0 \end{pmatrix}_{\mathbb{F}_2}$$

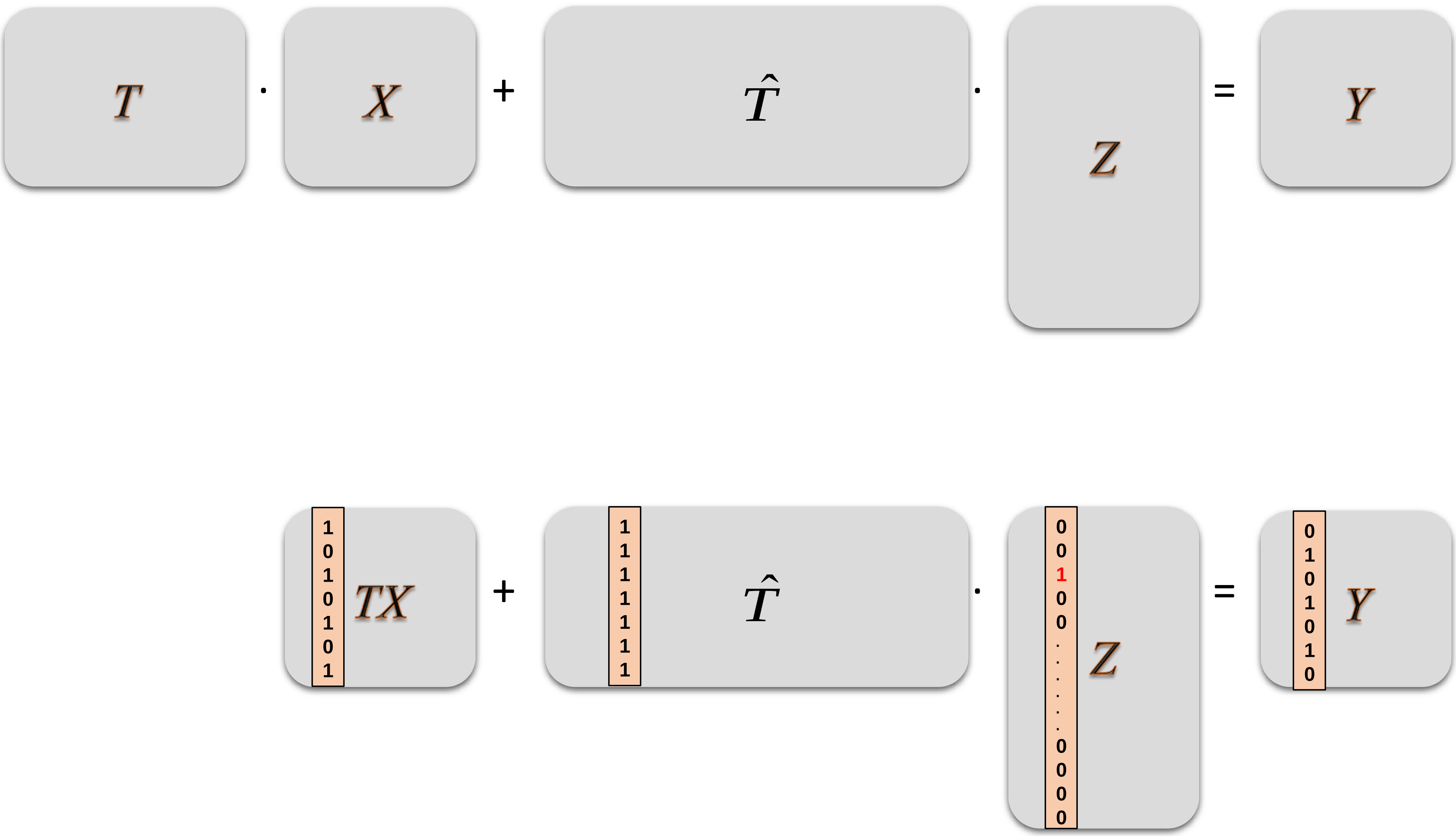
$$= \begin{pmatrix} 3 & 3 & 3 \\ 0 & 2 & 2 \end{pmatrix}_{\mathbb{F}_4}$$



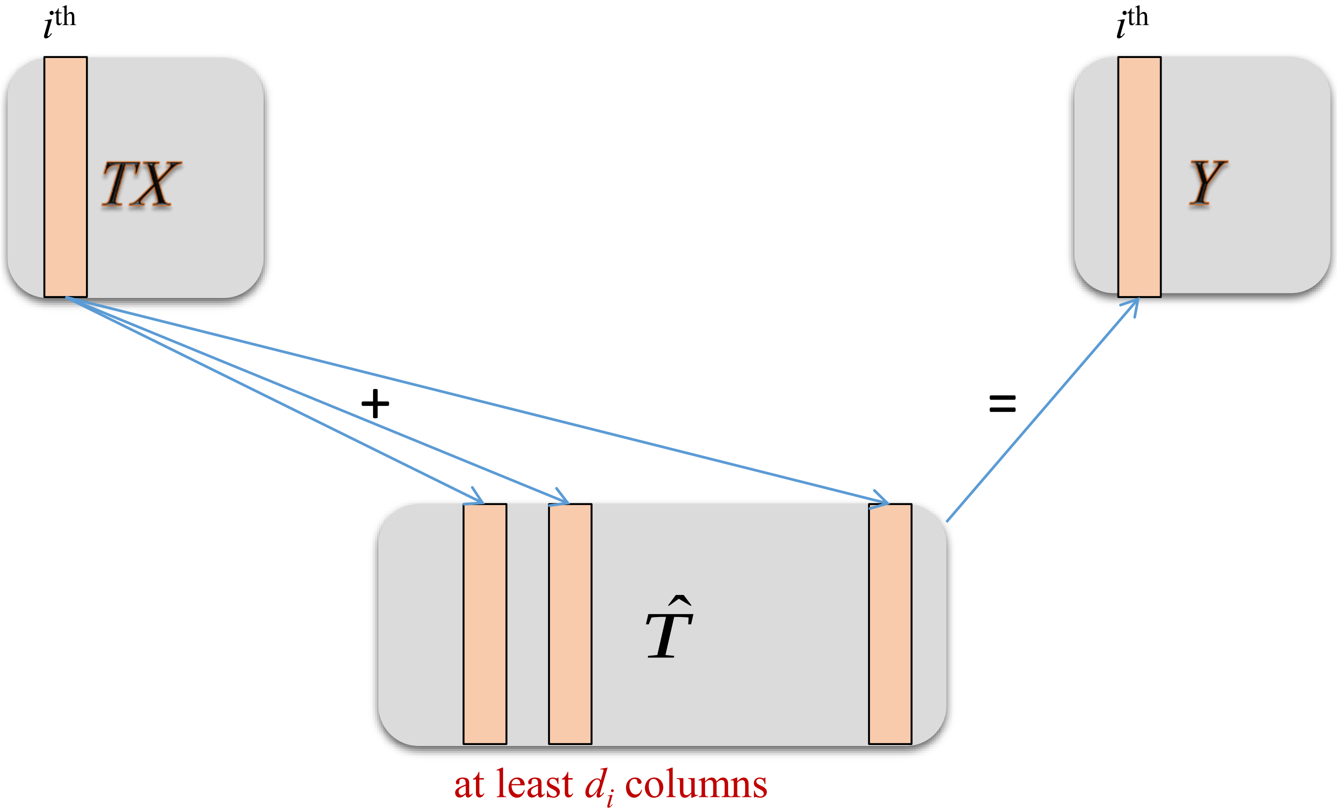
$$\left(\underset{Cm \times Cm}{T} \cdot \underset{Cm \times n}{X} + \underset{Cm \times Em}{\hat{T}} \cdot \underset{Em \times n}{Z} = \underset{Cm \times n}{Y} \right)_{\mathbf{F}_2}$$



T · X + T̂ · Z = Y
TX + T̂ · Z = Y
0
0
1
0
1
. . . .
0
0
1
0

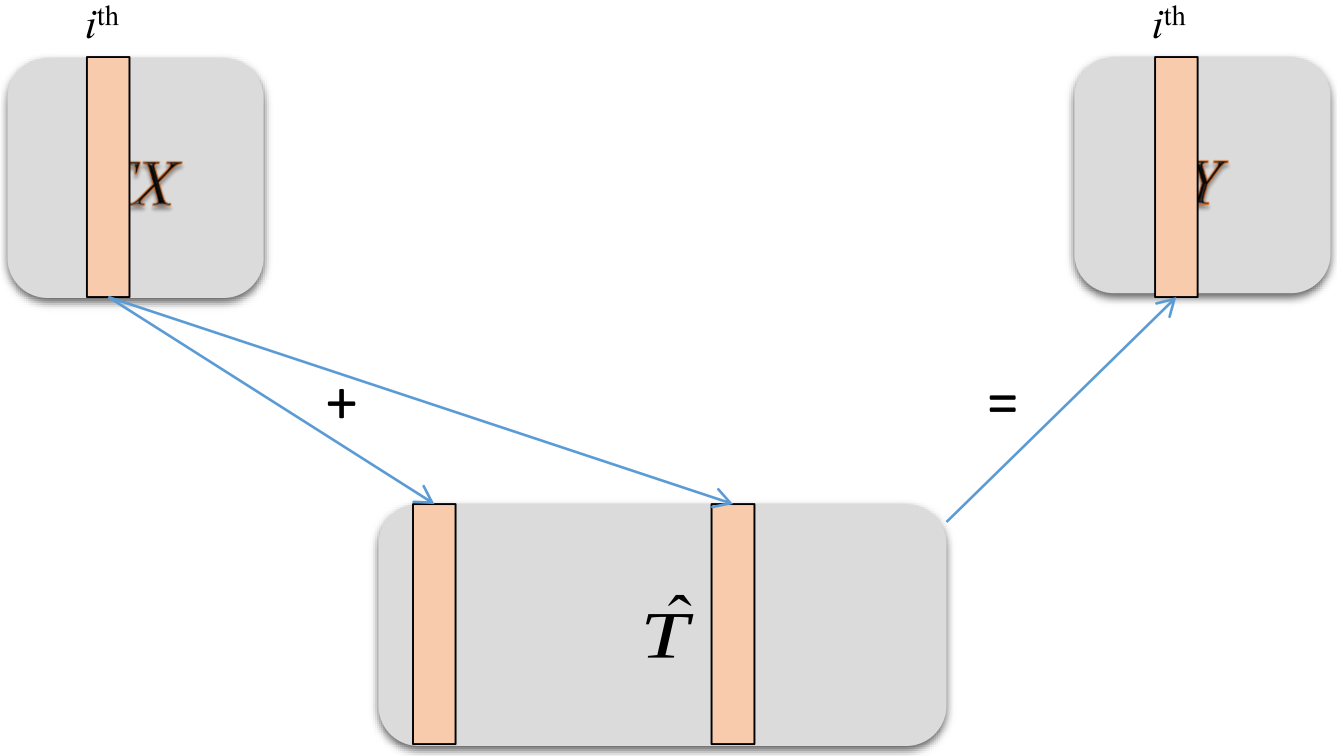

$T \cdot X + \hat{T} \cdot Z = Y$
1 0 1 0 1 0 1
TX
+
1 1 1 1 1 1 1
$\hat{T}$
·
0 0 1 0 0 . . . . . 0 0 0 0
Z
=
0 1 0 1 0 1 0
Y

Transform Metric

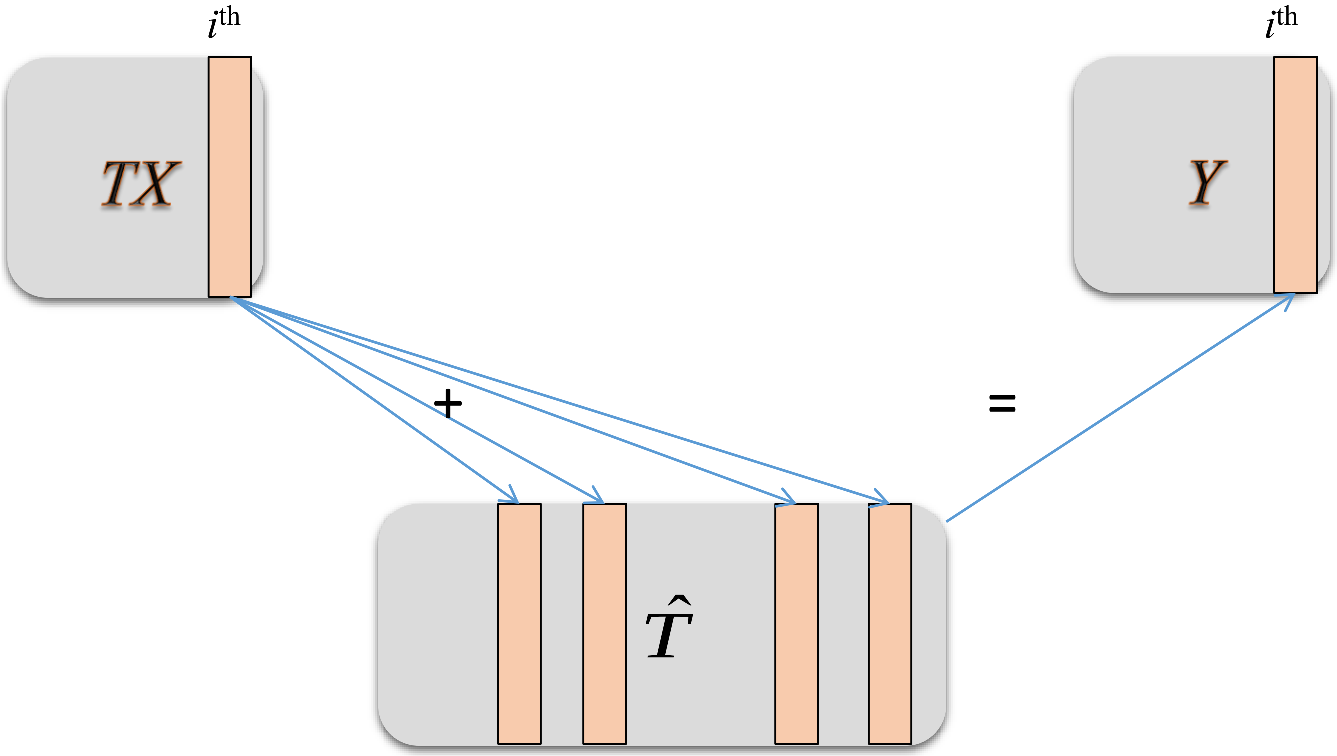


Claim: d_i is a distance metric.

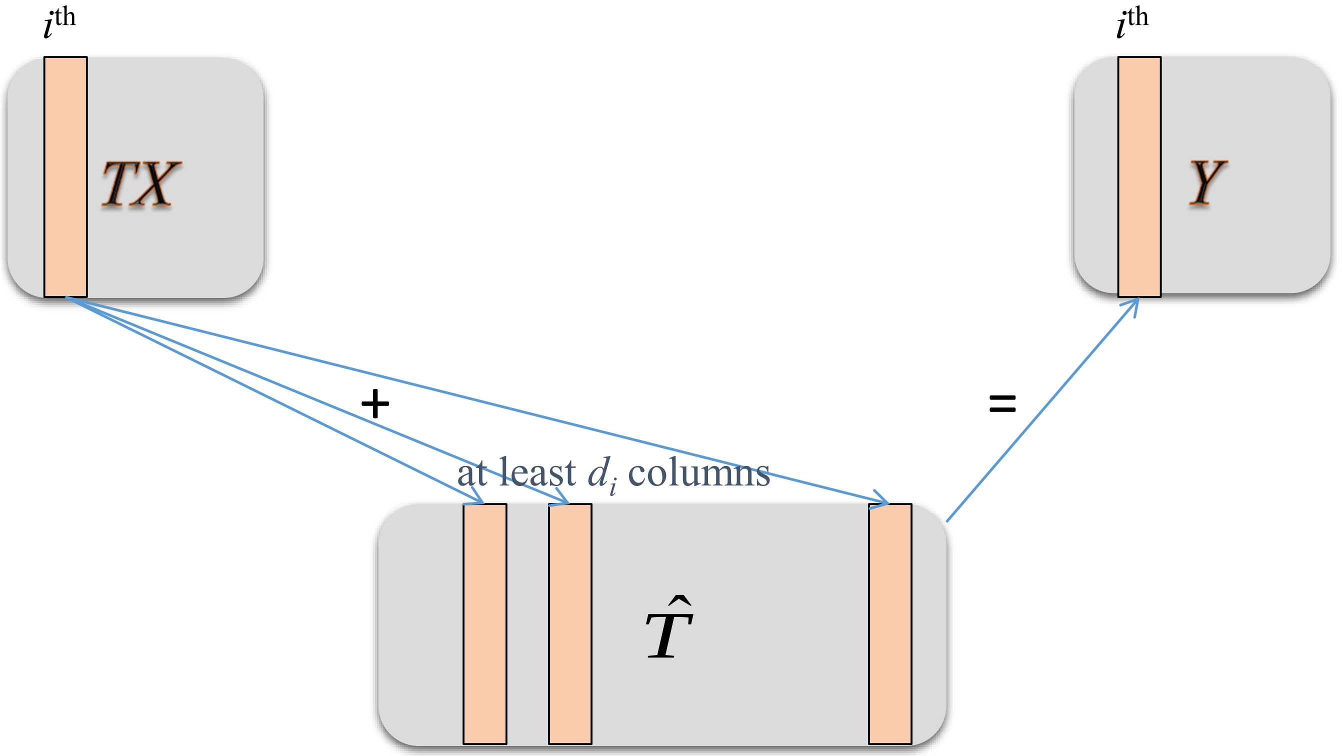
Transform Metric



Transform Metric



Transform Metric



$$d_{\hat{T}}(TX, Y) = \sum_{i=1}^{n} d_i$$

Claim: $d_{\hat{T}}(TX, Y)$ is a distance metric.

Main Results

Achievable schemes:

Gilbert-Varshamov

- *Coherent* GV-type codes achieve rates at least

$$1-\frac{E}{C}H(2p)$$

- *Non-coherent* GV-type codes achieve rates at least

$$1-\frac{E}{C}H(2p)$$

$2^{O(n)}$

Zyablov

- Concatenated network codes achieve rates at least

$$\max_{0<r<1-\frac{E}{C}H(2p)} r\cdot\left(1-\frac{2p}{H^{-1}\left(\frac{C}{E}(1-r)\right)}\right)$$

$n^{O(1)}$

Converses:

Hamming

- For all $p<\frac{C}{2Em}$

$$R\leq 1-\frac{E}{C}H(p)$$

Plotkin

- For all $p<\frac{C}{E}(1-\frac{C}{E})$

$$R\leq 1-\frac{E^2}{CE-C^2}p$$

- If $p\geq\frac{C}{E}(1-\frac{C}{E})$

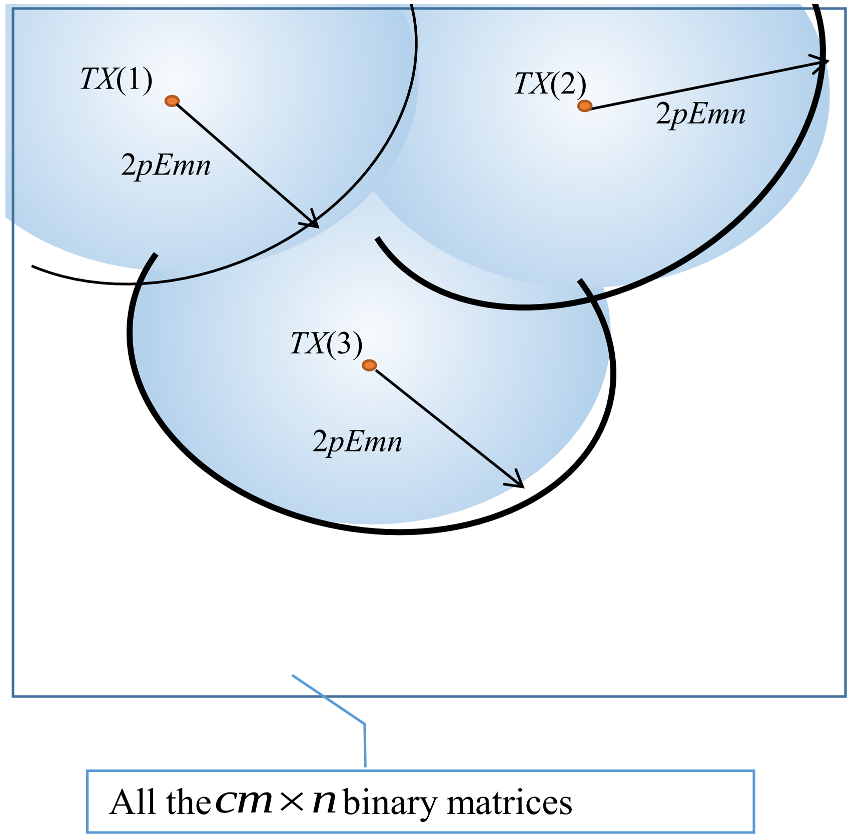
$$R=0$$

Elias-Bassalygo

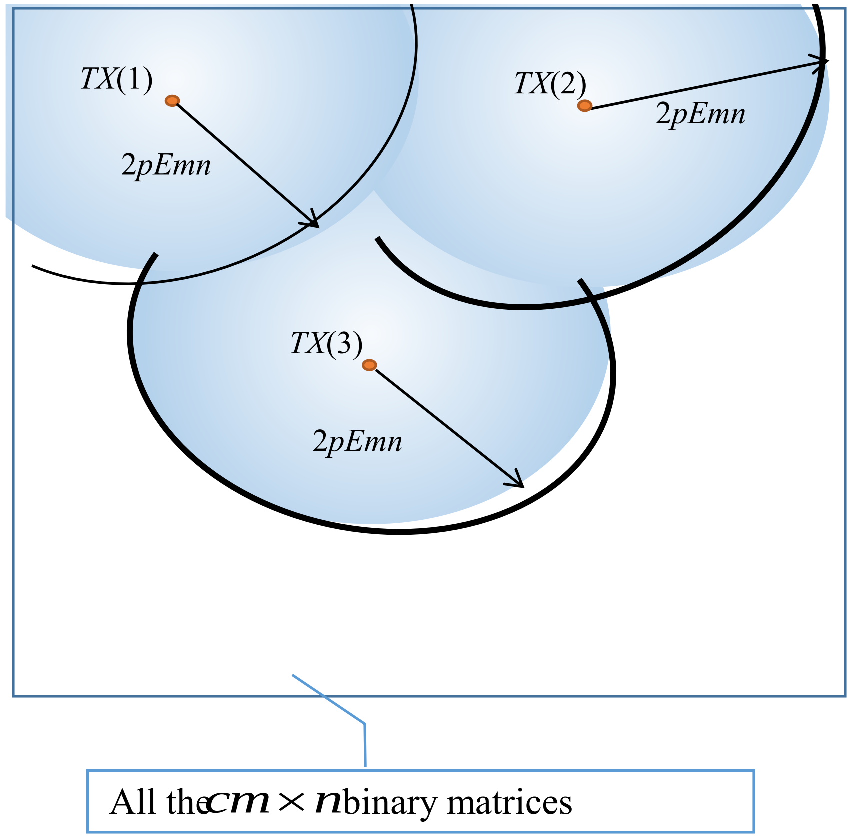
- For all $p<\frac{C}{2Em}(1-\frac{C}{2Em})$

$$R<1-\frac{E}{C}H\left(\frac{1-\sqrt{1-4p}}{2}\right)$$

Gilbert-Varshamov-Type Bound (coherent)



Gilbert-Varshamov-Type Bound (coherent)



- Need an **upper bound** on volume of

$$B_{\hat{T}}(TX, 2pEmn)$$

- **Different Y**, or equivalently $\hat{T}Z$, can be **bounded above** by the number of **different Z**, which equals

$$\sum_{i=0}^{2pEmn} \binom{Emn}{i}$$

- The summation can be bounded from above by

$$(2pEmn+1)\binom{\tilde{E}mn}{2pEmn} \qquad (2pEmn+1)2^{H(2p)Emn}$$

- **Lower bound** on the size of the codebook

$$\frac{2^{Cmn}}{(2pEmn+1)2^{H(2p)Emn}} = 2^{(1-\frac{E}{C}H(2p)-\frac{\log(2pEmn+1)}{n})Cmn}$$

- Asymptotically in *n*, the rate of coherent GV-type codes

$$1-\frac{E}{C}H(2p)$$

Unknown knowns part III:
Arbitrarily Varying Networks

Peida Tian

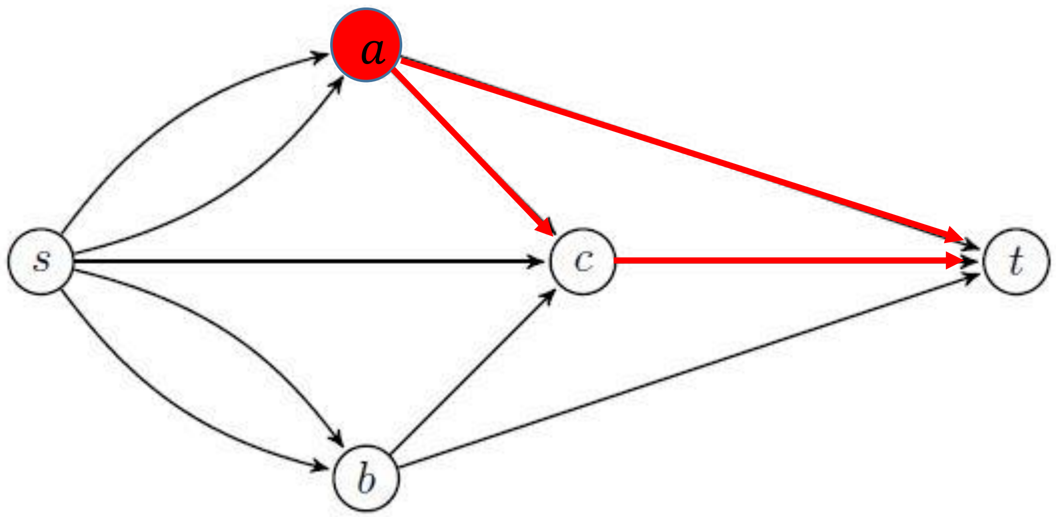
Sidharth Jaggi

Oliver Kosut

Background – Related Work

Node-based jamming adversary

- Calvin: eavesdrop on all links
- jam on outgoing links of any z nodes
- Goal: ***reliable*** communication

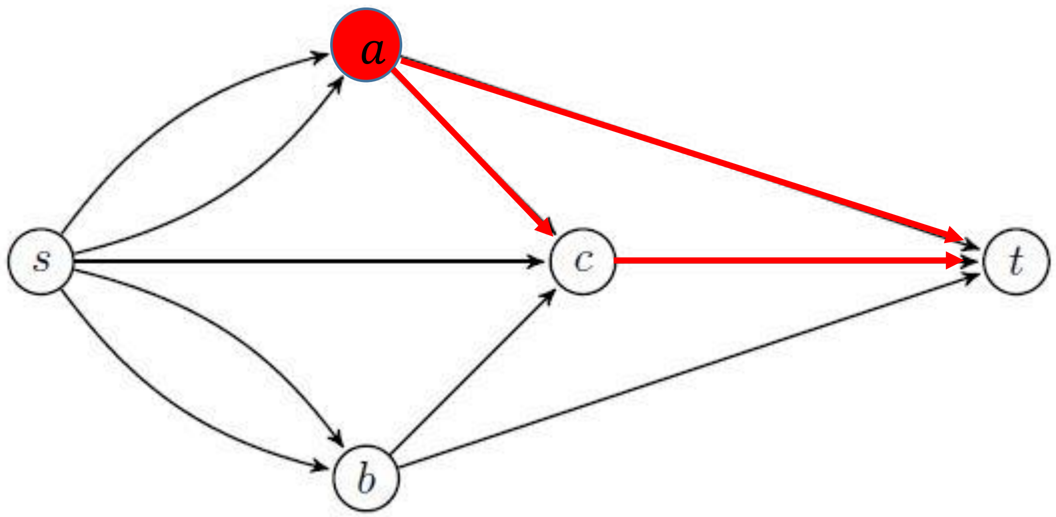


Upper bound:
- Bounds from link-based adversary (too pessimistic)
- cut-set bound [Kosut et al] (not tight in general)

Lower bound (achievability):
- routing bounds [Che et al] (unicast)
- Polytope codes [Kosut et al]

Shared secrets – "Arbitrarily Varying Networks"

- Calvin: eavesdrop on all links
- jam on outgoing links of any z nodes
- Goal: ***reliable*** communication
  - How about negligible ***shared secrets*** between source and every nodes



Higher rate possible

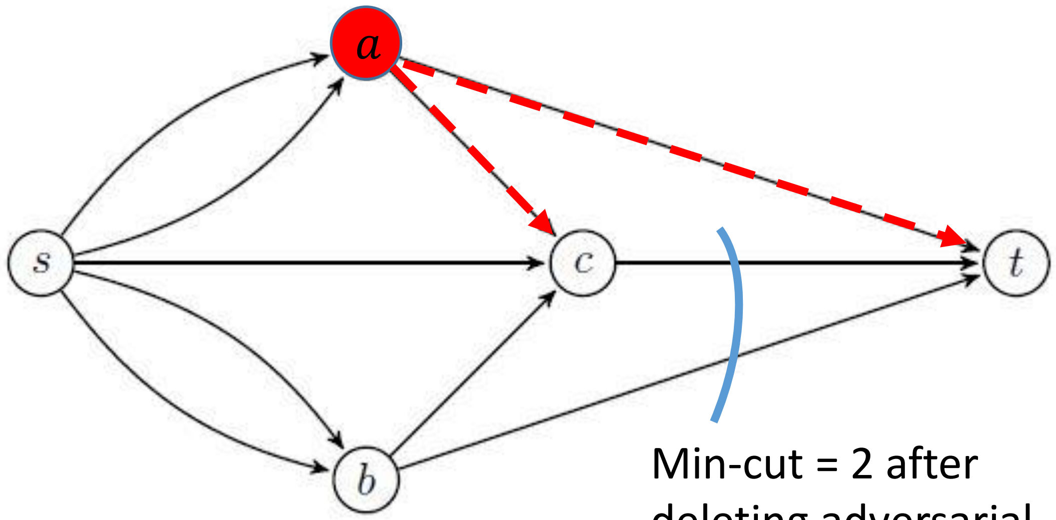
Shared secrets – “Arbitrarily Varying Networks”

Capacity: natural “erasure” outer bound

Code strategy:

- Authenticate packets
- Intermediate nodes verify and delete corrupted packets

Challenge



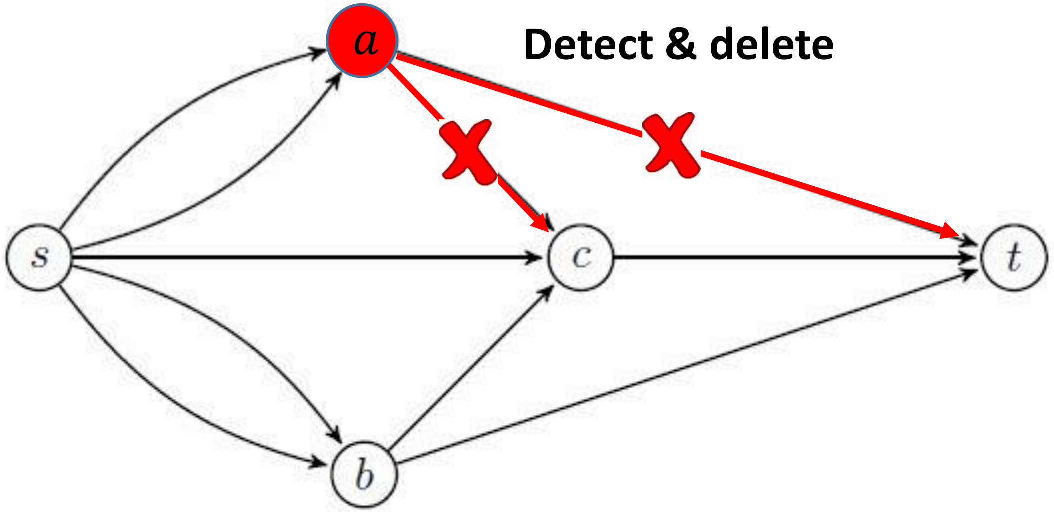
Min-cut = 2 after deleting adversarial node

Shared secrets – "Arbitrarily Varying Networks"

Idea:
Verify any linear combination
$aX_1 + bX_2$ using hashes from X_1, X_2

Key tool:
hash function $h(\cdot)$ based on
linearized polynomial

Our code:
Computationally efficient
rate optimal



Shared secrets – "Arbitrarily Varying Networks"

Sketch of hash functions

$h(X_1, s_1) = s_{12} + \sum_{k=1}^{n} x_{1k} s_{11}^{p^k}$ $h(X_2, s_2) = s_{22} + \sum_{k=1}^{n} x_{2k} s_{21}^{p^k}$

$h(aX_1 + bX_2, s_1)$ can be computed using $h(X_1, s_1), h(X_1, s_2), h(X_2, s_1), h(X_2, s_2)$

- Properties of linearized polynomial
- Schwartz-Zippel Lemma

Less well-understood

Unknowns…

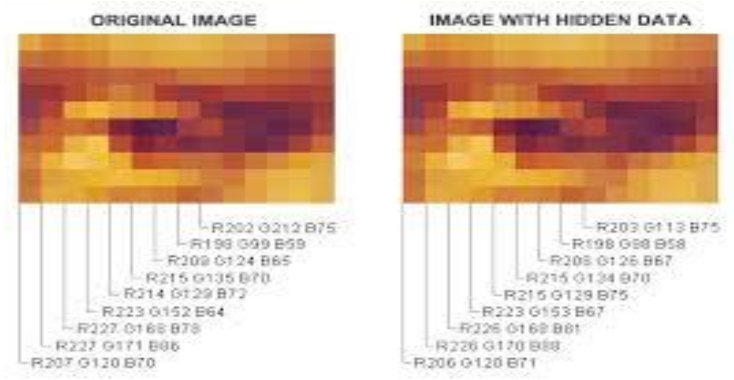
At least to me…

Layers of secrecy

Anonymity

"Who is hiding something?"

Deniability/
Steganography

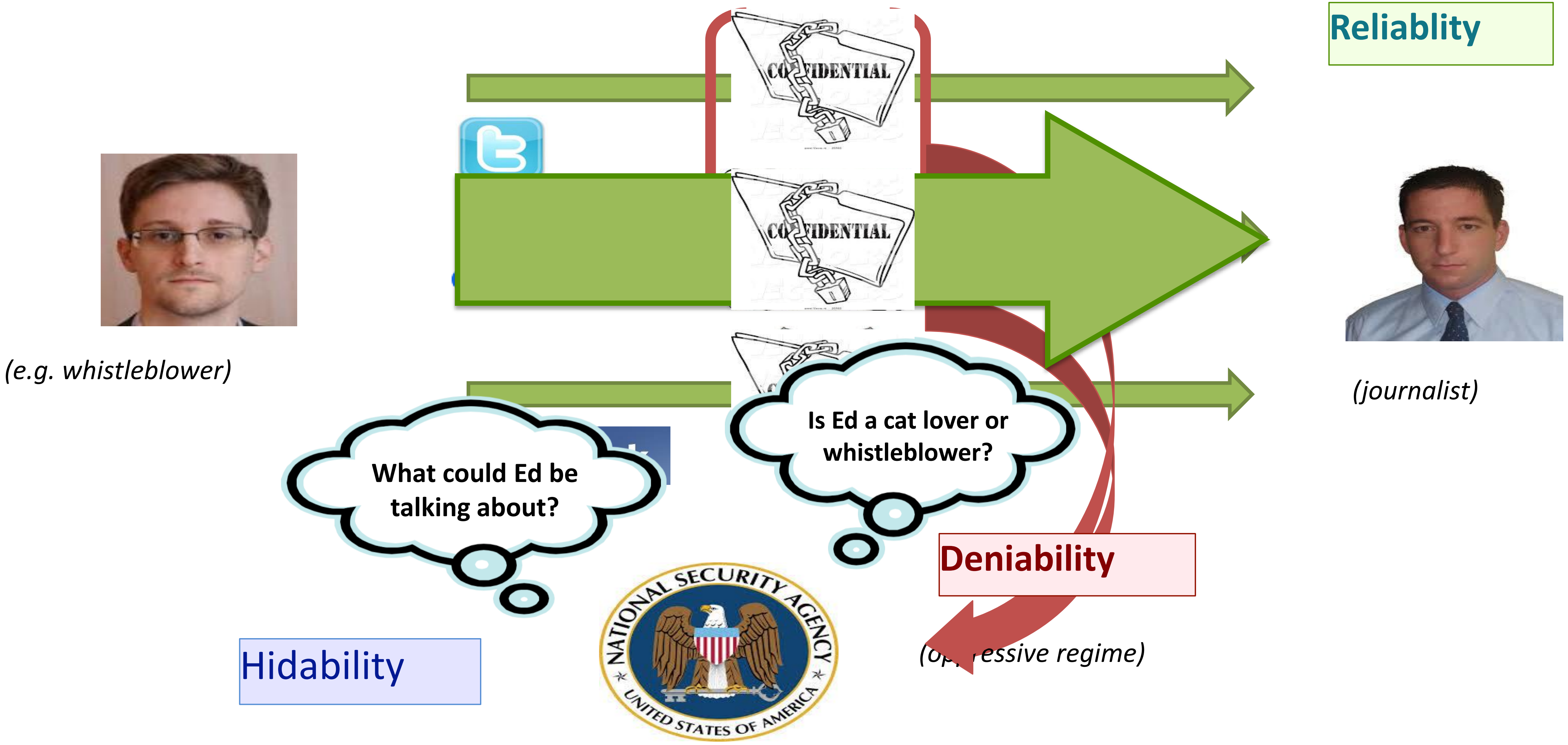


"Is s/he hiding something?"

Secrecy
(IT or crypto)

"What is s/he hiding?"

Motivating Scenario



Layers of robustness

- Network-error correction – what is s/he saying?
- Network function computation – what does s/he mean?
- Network tomography – who’s messing with us?

Future work…

謝謝