

# Extractors

Low Entropy Requirements Colliding  
with Non-Malleability

Divesh

Eldon

Maciej

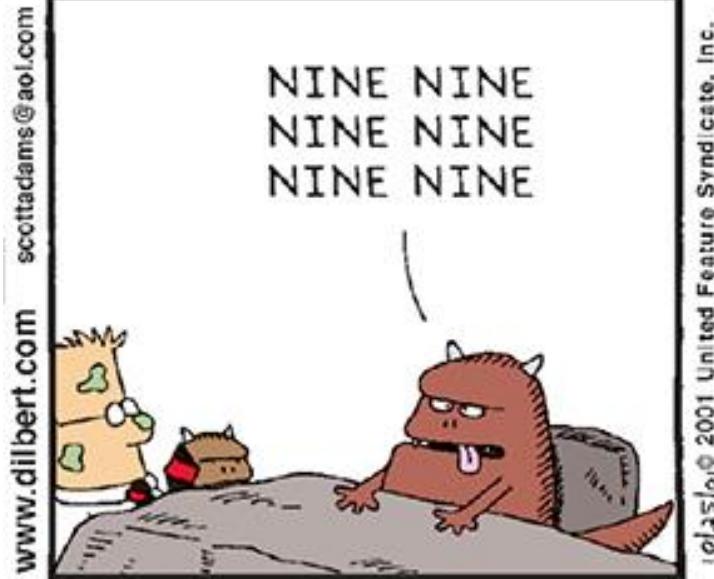
Aggarwal

Chung

Obremski

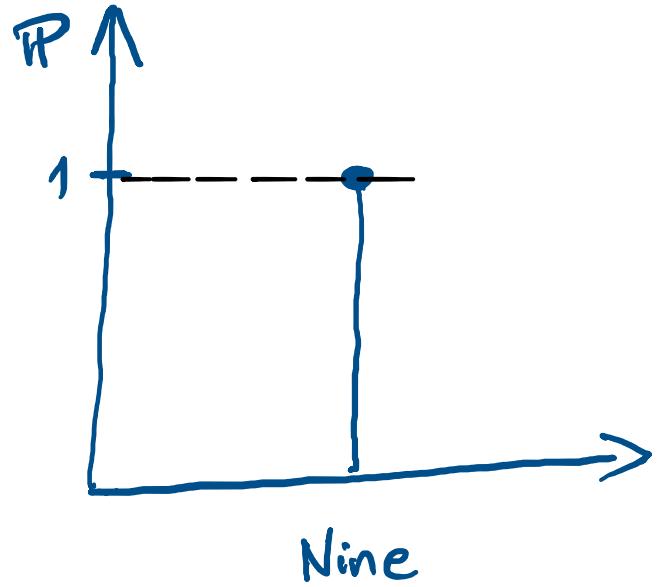
National University of Singapore

# Randomness



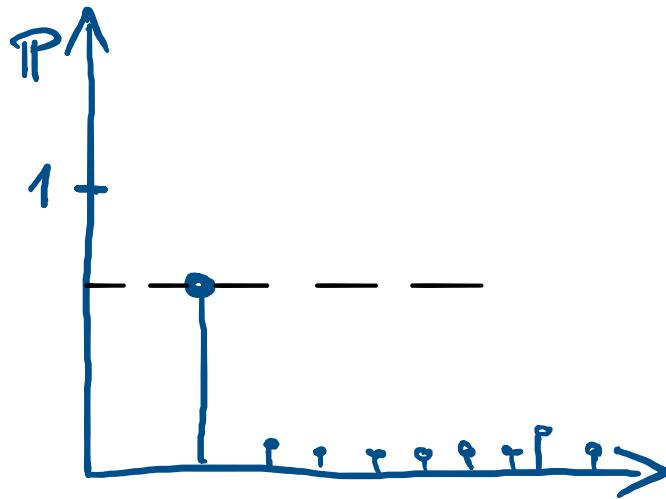
All processes are random  
but some processes are  
more random than others.

## Min-Entropy



$$H_{\infty}(X) = -\log \max_x P(X=x)$$

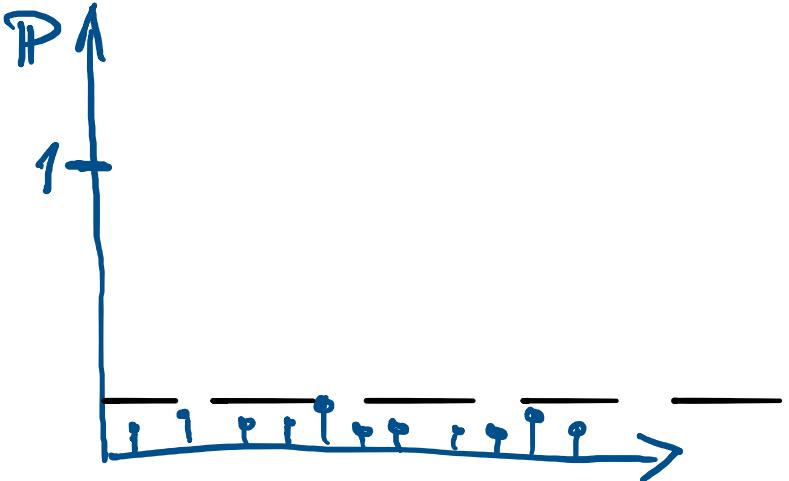
Nine



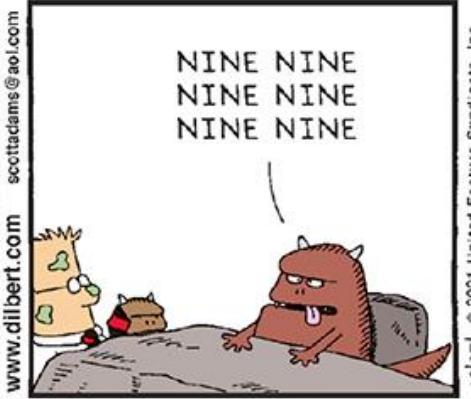
$$X \sim \text{uniform } \{0, 1\}^n$$

$$H_{\infty}(X) = n$$

this is  
maximum  
possible.



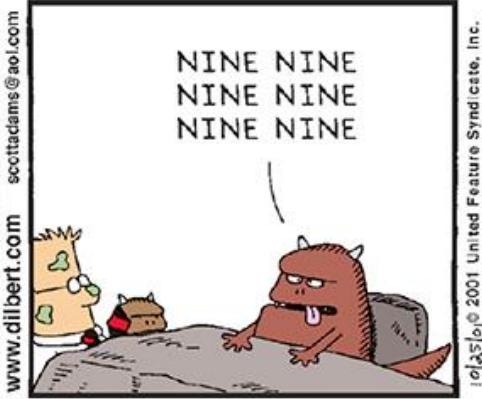
# Extractors



?



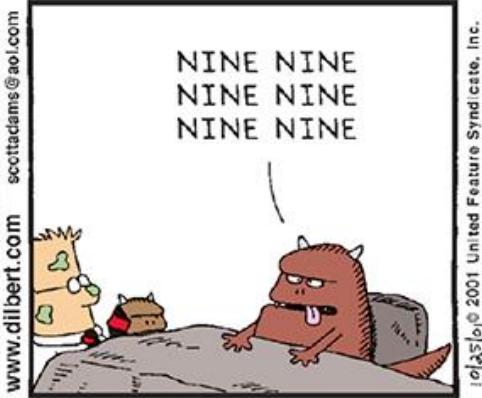
# Extractors



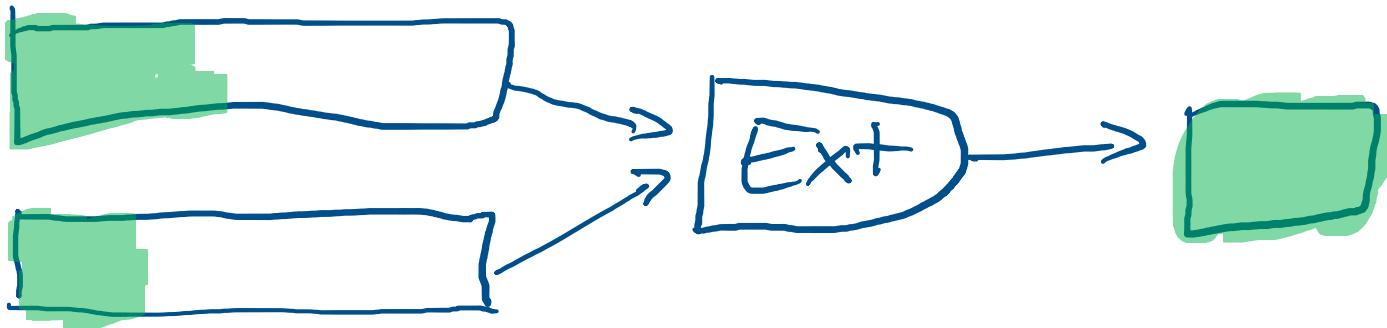
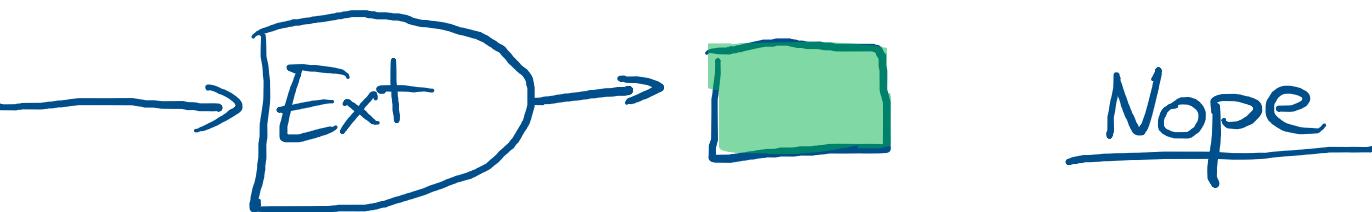
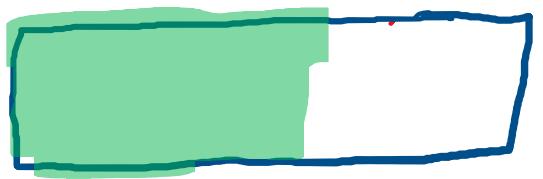
?



# Extractors

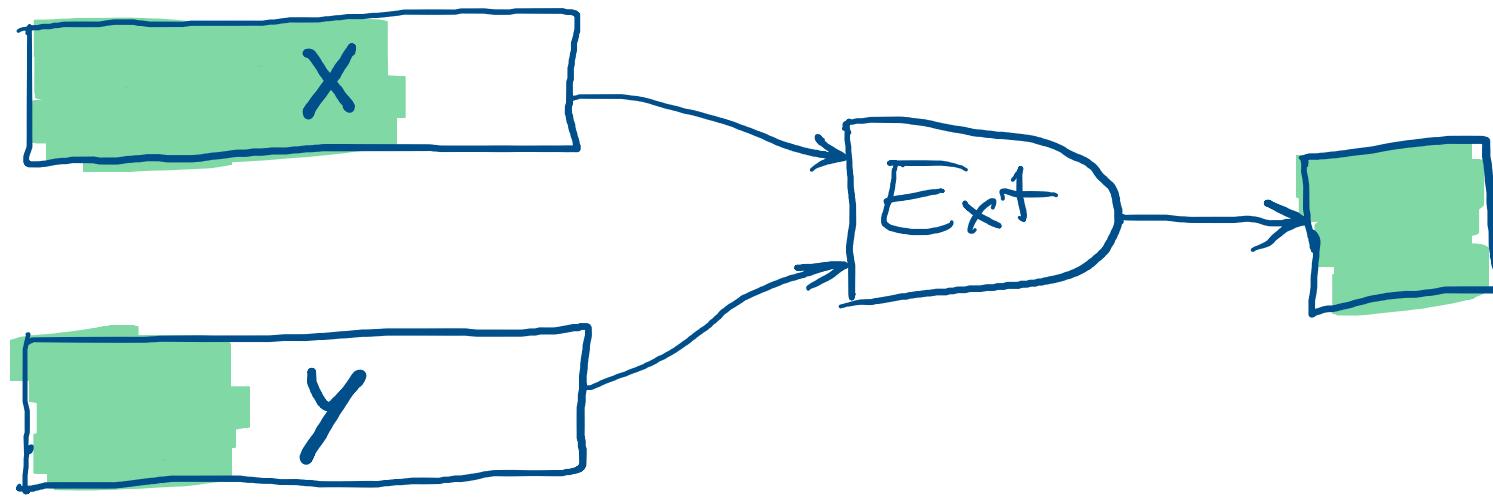


?

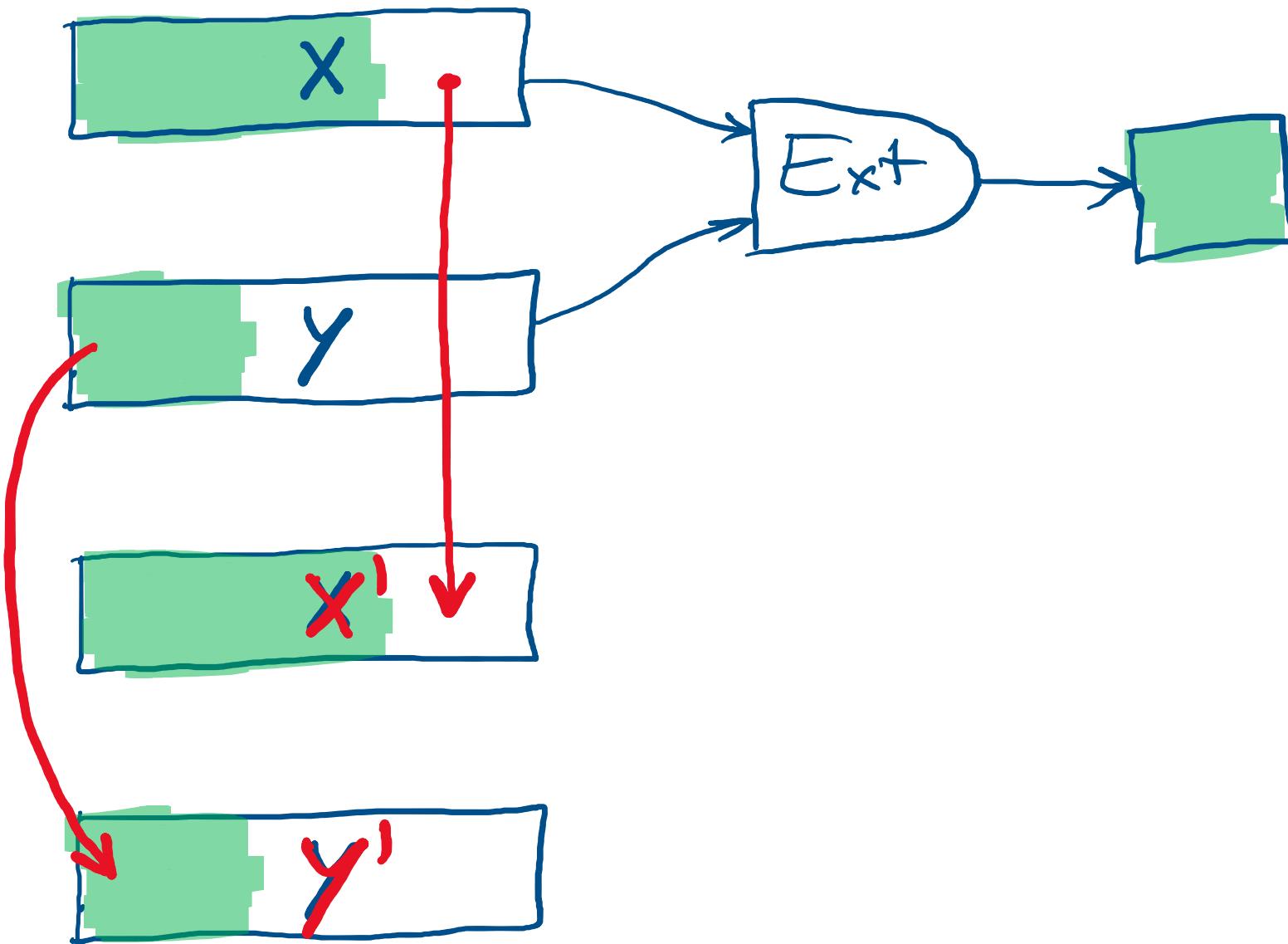


Yay

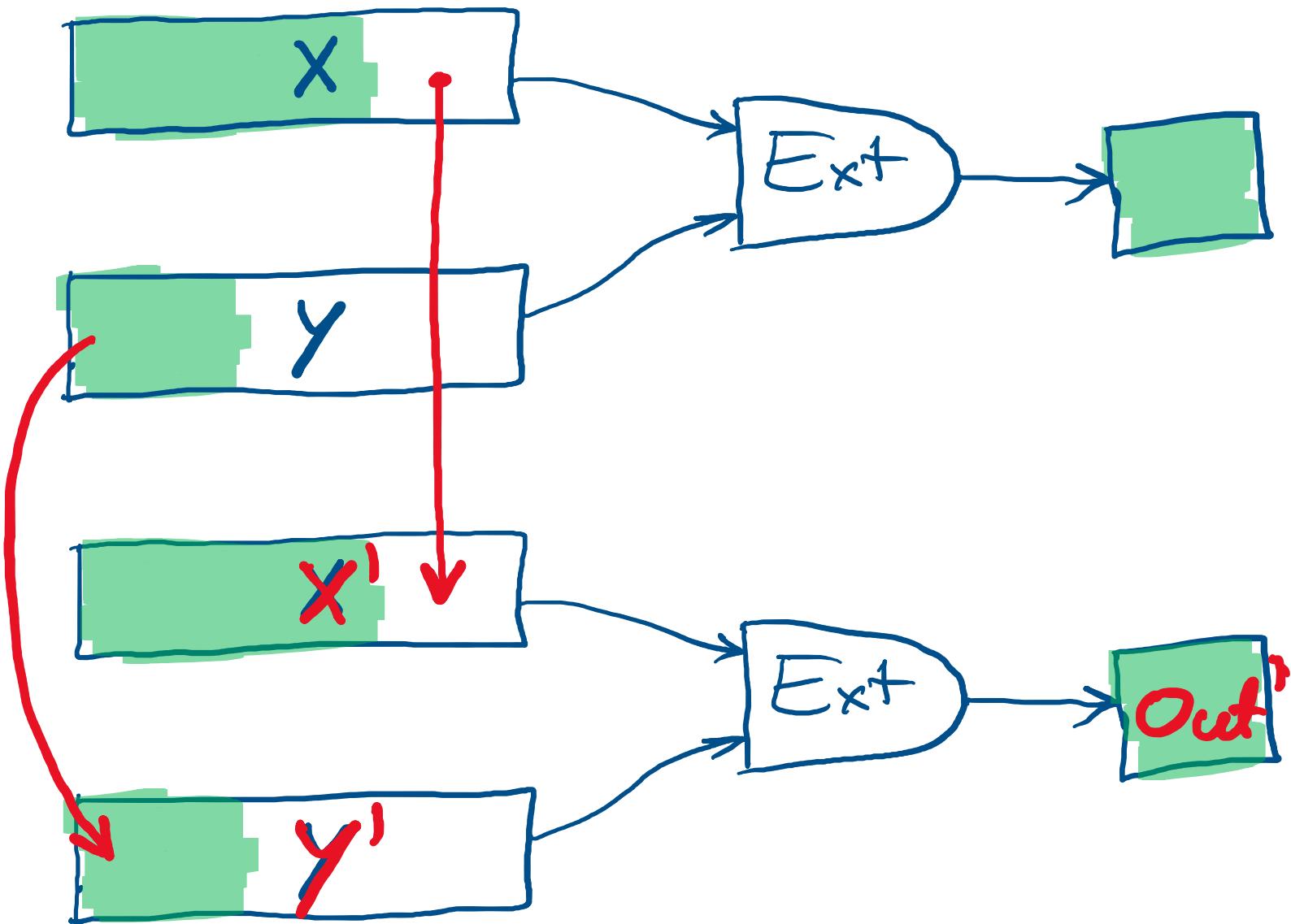
# Non-Malleability



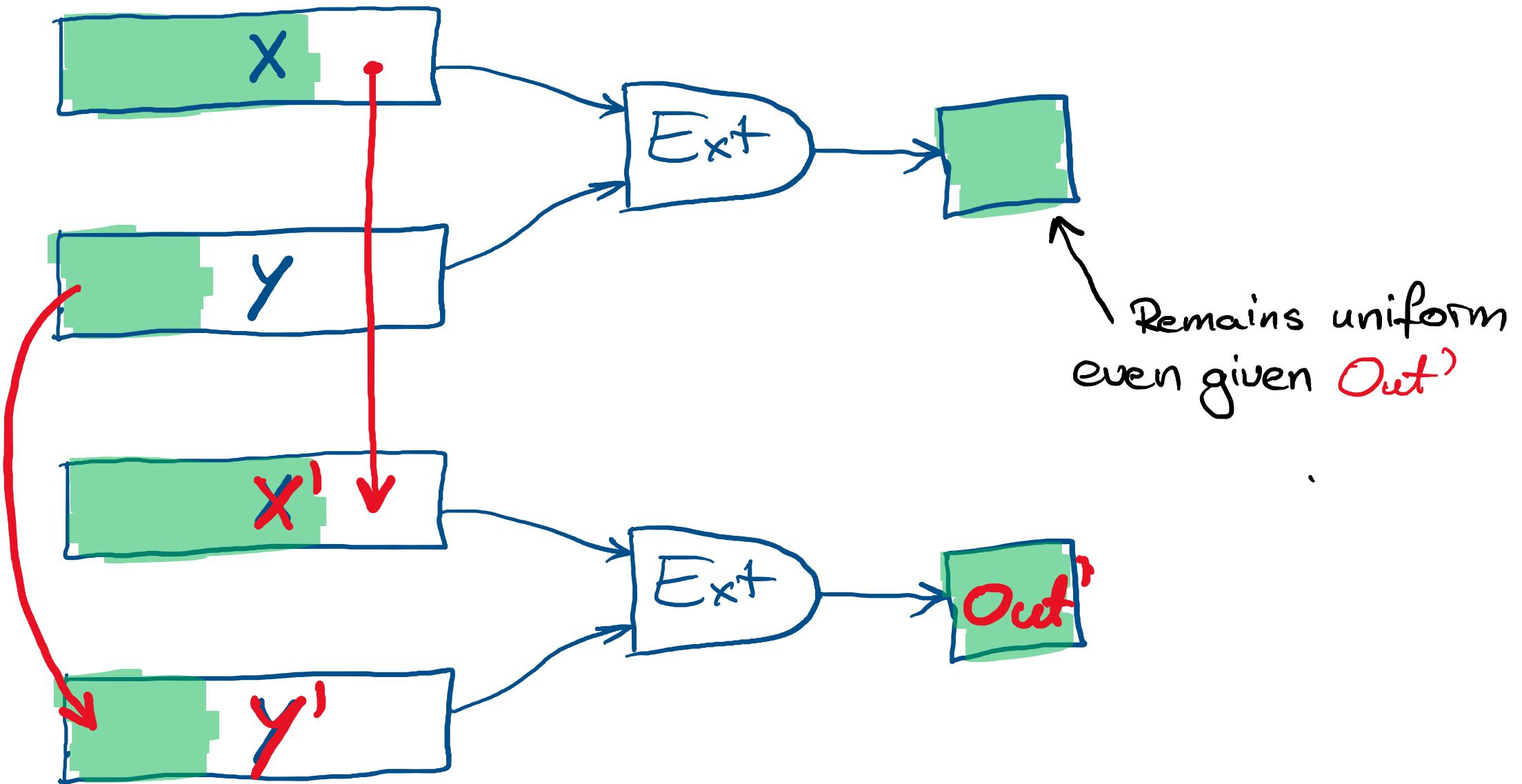
# Non-Malleability



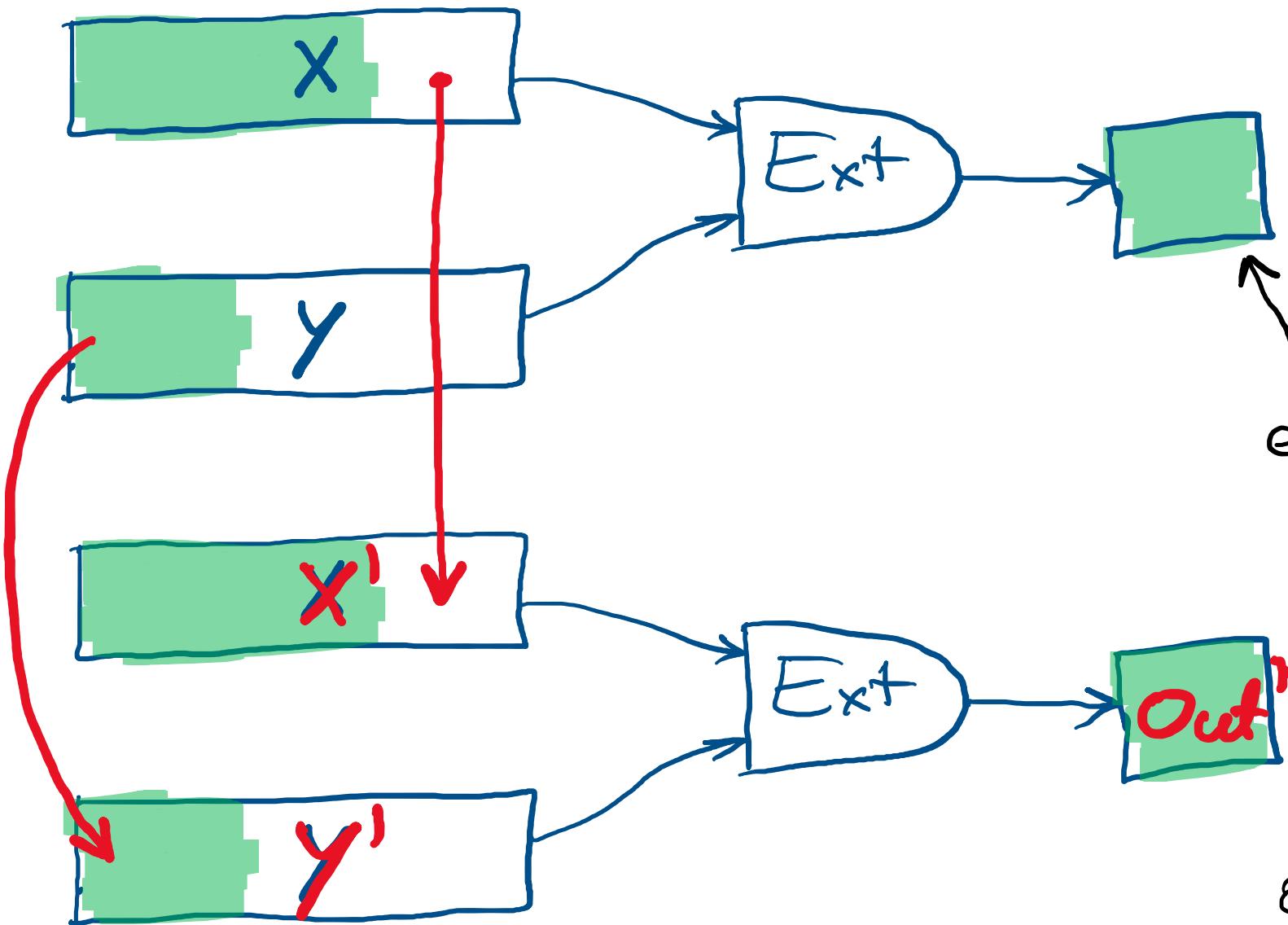
# Non-Malleability



# Non-Malleability



# Non-Malleability



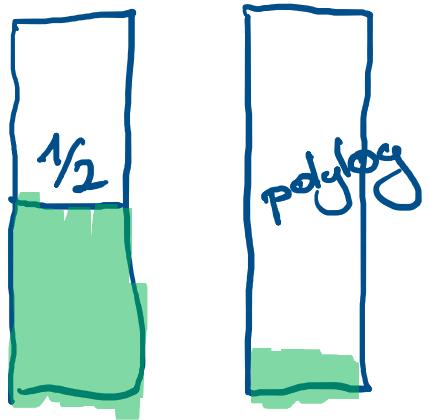
Remains uniform  
even given **Out'**

Even if,  
**X** and **X'** are  
correlated,  
and **Y**, **Y'** are  
correlated  
**Out** and **Out'** are  
Independent.

What we know (negligible error)

## What we know (negligible error)

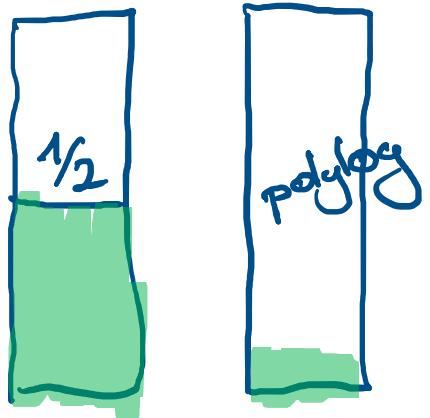
Raz



Not  
NM

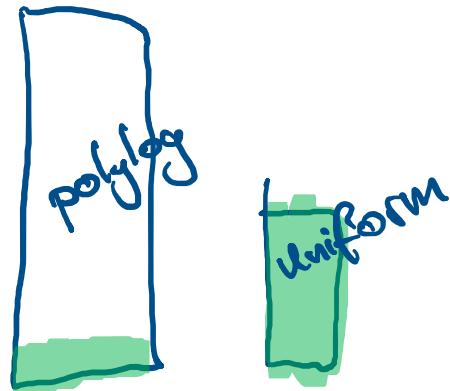
## What we know (negligible error)

Raz



Not  
NM

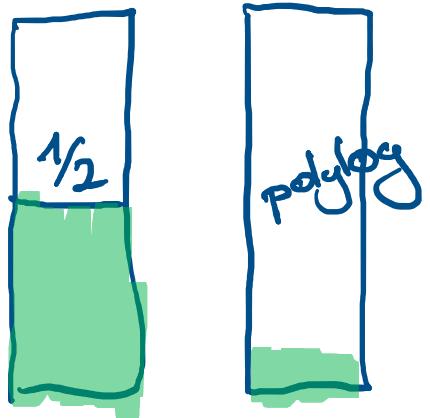
Seeded nMExt



NM with  
respect to  
seed

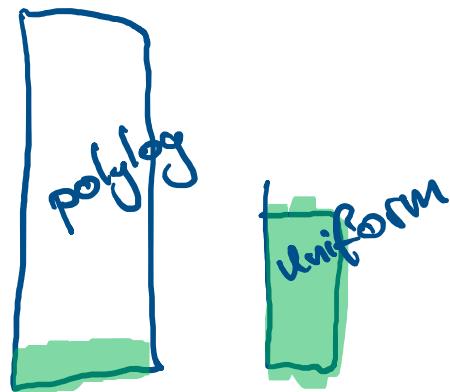
# What we know (negligible error)

Raz



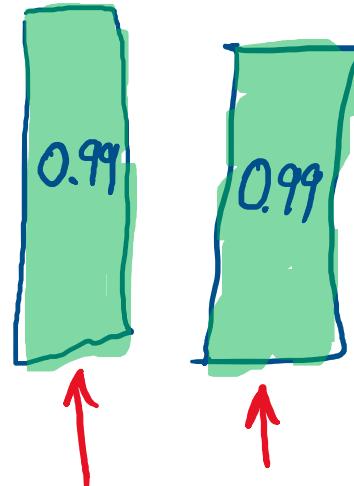
Not NM

Seeded nmExt



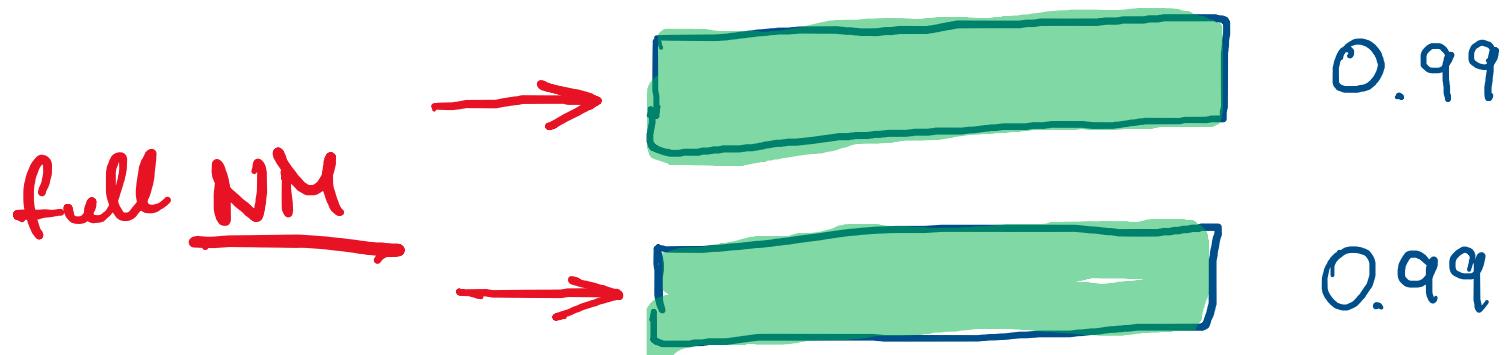
↑  
NM with respect to seed

2 nmExt

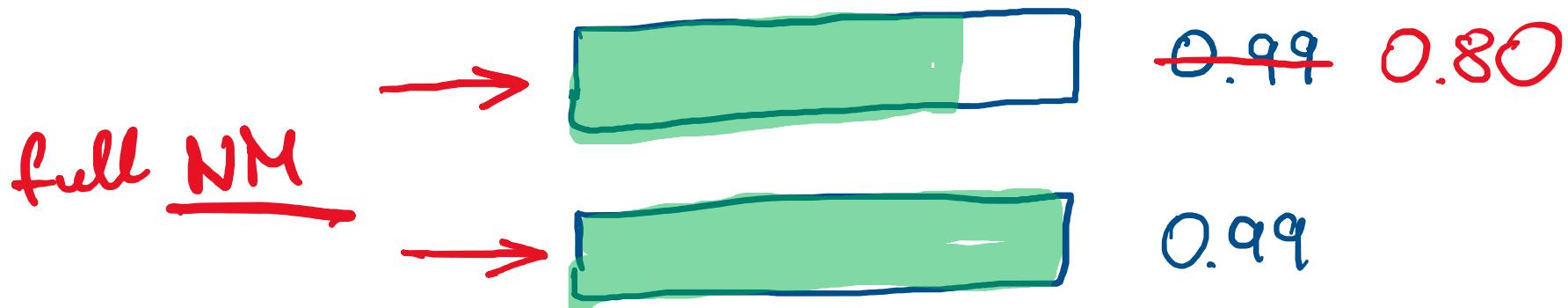


full NM

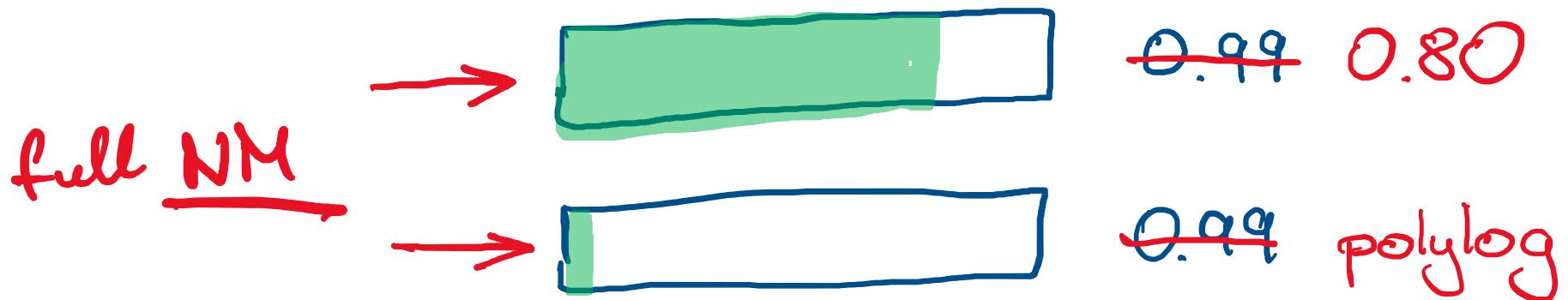
## What we know NOW



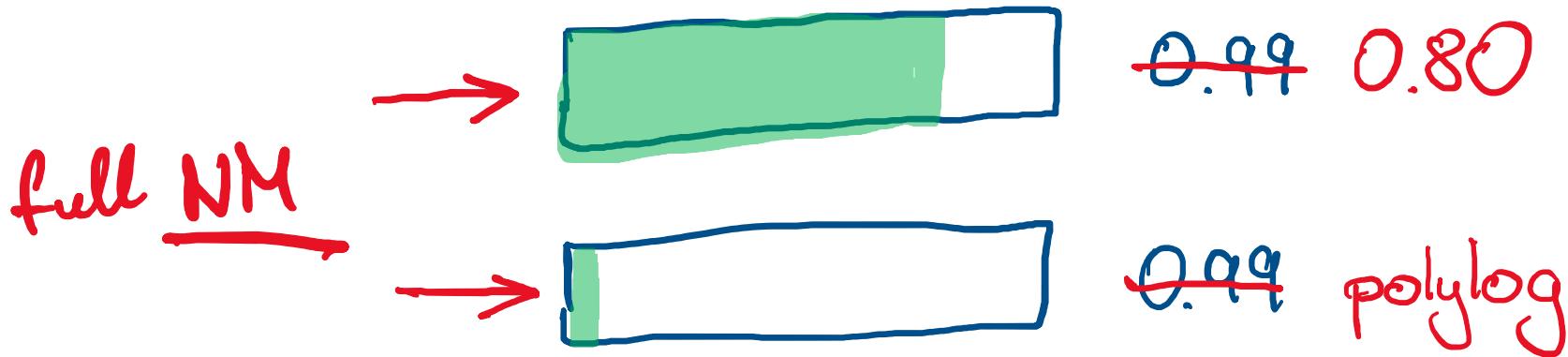
## What we Know NOW



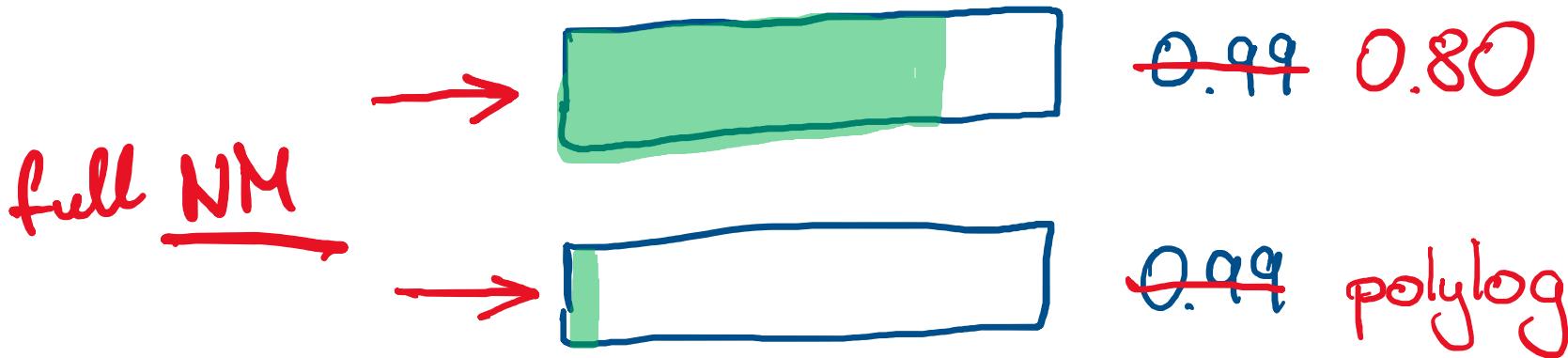
## What we know NOW



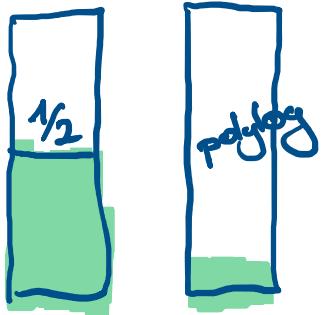
## Best of all Worlds



## Best of all Worlds

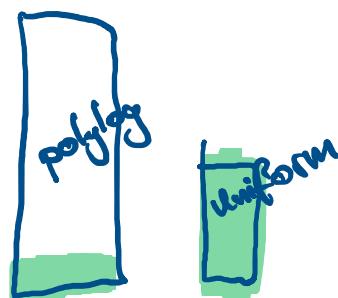


Raz



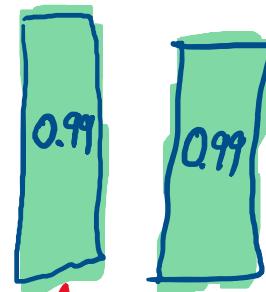
Not NM

Seeded nmExt



NM with  
respect to  
Source

2 nmExt



full NM

## A bit more history

Goyal, Srinivasan, Zhu '21 considered following

$$2\text{NMExt}(\boxed{X}, \boxed{Y_1 \amalg Y_2}) =$$

## A bit more history

Goyal, Srinivasan, Zhu '21 considered following

$$2\text{NMExt}(\boxed{X}, \boxed{Y_1 \amalg Y_2}) = \text{Li}\left( ; \boxed{Y_2} \right)$$

## A bit more history

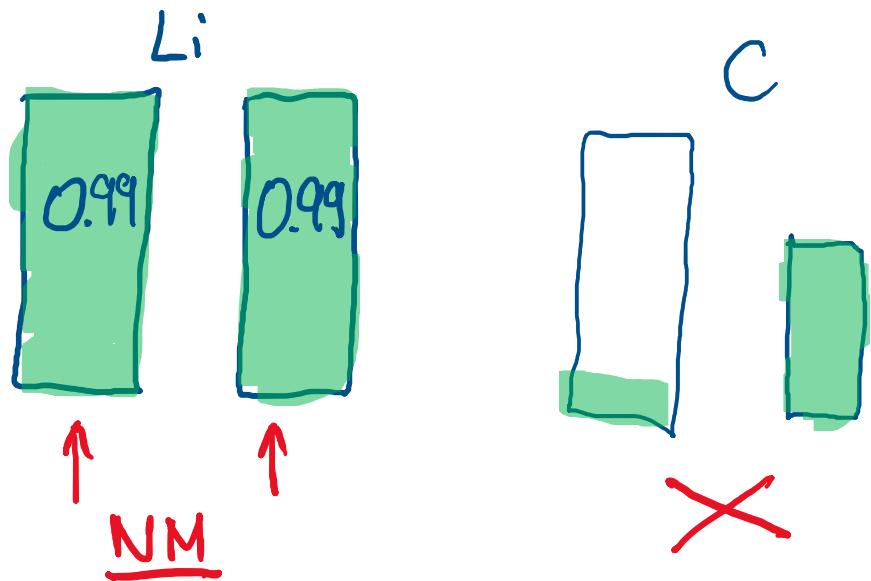
Goyal, Srinivasan, Zhu '21 considered following

$$2\text{NMExt}(\boxed{X}, \boxed{Y_1 \parallel Y_2}) = \text{Li} \left( C(\boxed{X}, \boxed{Y_1}); \boxed{Y_2} \right)$$

## A bit more history

Goyal, Srinivasan, Zhu '21 considered following

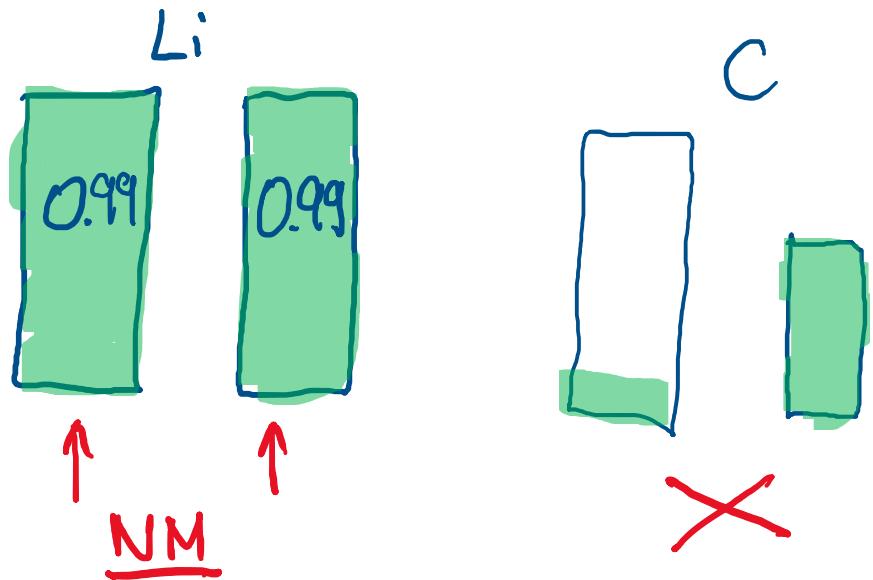
$$2NM \text{Ext}(\boxed{X}, \boxed{Y_1 \parallel Y_2}) = \text{Li} \left( C(\boxed{X}, \boxed{Y_1}); \boxed{Y_2} \right)$$



## A bit more history

Goyal, Srinivasan, Zhu '21 considered following

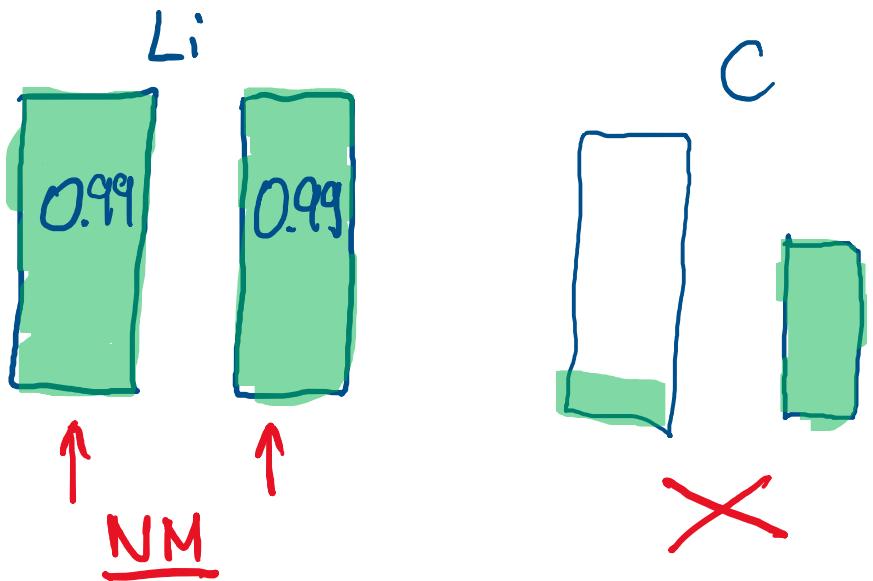
$$2NM \text{Ext}(\boxed{X}, \boxed{Y_1 \parallel Y_2}) = \text{Li} \left( C(\boxed{X}, \boxed{Y_1}); \boxed{Y_2} \right)$$



## A bit more history

Goyal, Srinivasan, Zhu '21 considered following

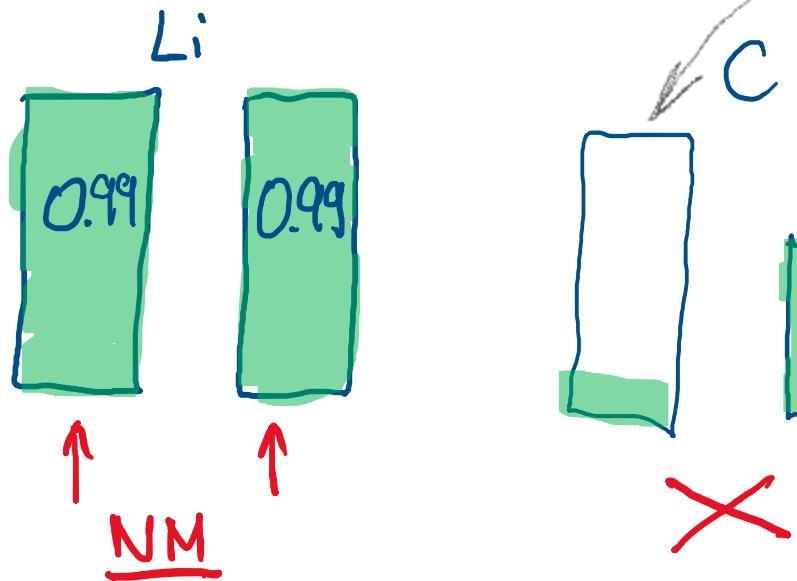
$$2NM \text{Ext}(\boxed{X}, \boxed{Y_1 \parallel Y_2}) = \text{Li} \left( C(\boxed{X}, \boxed{Y_1}); \boxed{Y_2} \right)$$



## A bit more history

Goyal, Srinivasan, Zhu '21 considered following

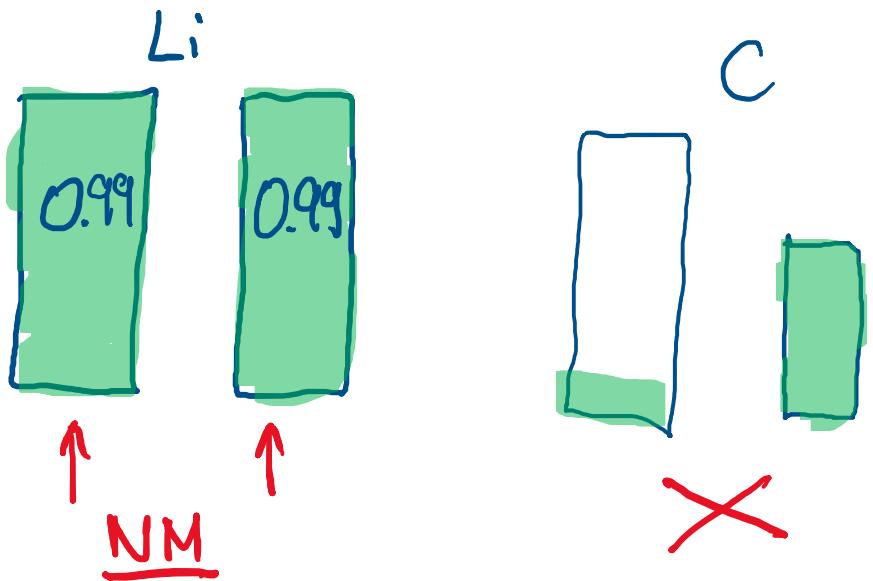
$$2NM \text{Ext}(\boxed{X}, \boxed{Y_1 \parallel Y_2}) = \text{Li} \left( C(\boxed{X}, \boxed{Y_1}); \boxed{Y_2} \right)$$



## A bit more history

Goyal, Srinivasan, Zhu '21 considered following

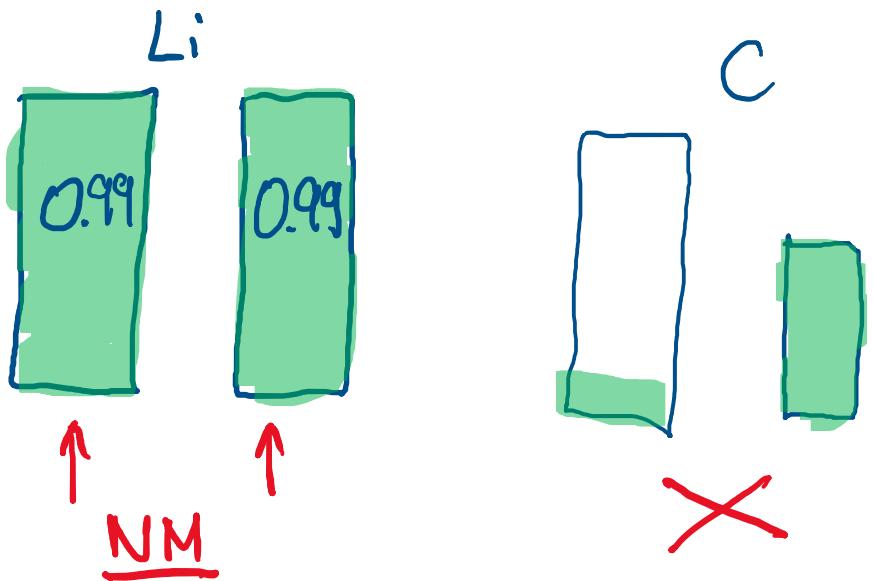
$$2NM \text{Ext}(\boxed{X}, \boxed{Y_1 \parallel Y_2}) = \text{Li} \left( C(\boxed{X}, \boxed{Y_1}); \boxed{Y_2} \right)$$



## A bit more history

Goyal, Srinivasan, Zhu '21 considered following

$$2NM \text{Ext}(\boxed{X}, \boxed{Y_1 \parallel Y_2}) = \text{Li} \left( C(\boxed{X}, \boxed{Y_1}); \boxed{Y_2} \right)$$



## A bit more history

Goyal, Srinivasan, Zhu '21 considered following

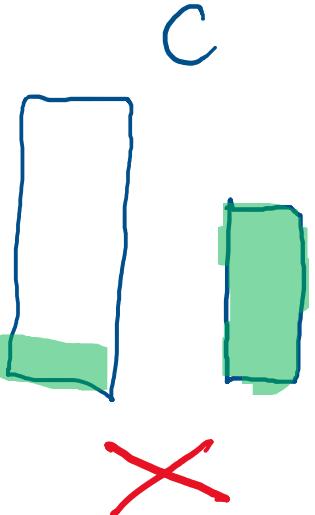
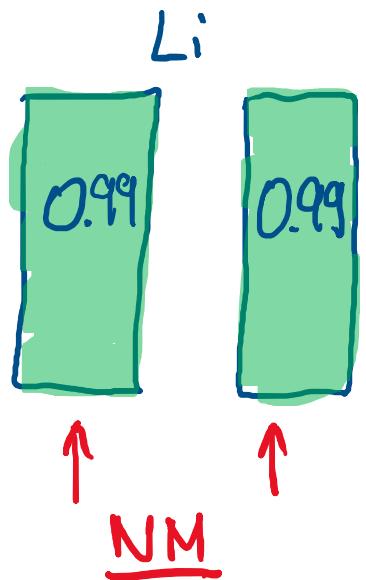
$$2NM \text{Ext}(\boxed{X}, \boxed{Y_1 \parallel Y_2}) = \text{Li} \left( C(\boxed{X}, \boxed{Y_1}); \boxed{Y_2} \right)$$

The diagram illustrates the components of the equation. It features two parallel stacks of rectangular boxes. The left stack, labeled 'Li', contains two boxes, each with the value '0.99' written inside. The right stack, labeled 'C', contains two boxes; the bottom one is crossed out with a large red 'X', while the top one remains. Arrows point from the 'Li' stack to the 'C' stack, and another arrow points from the 'C' stack towards the right side of the equation.

## A bit more history

Goyal, Srinivasan, Zhu '21 considered following

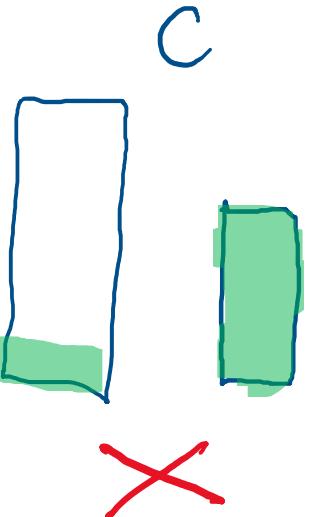
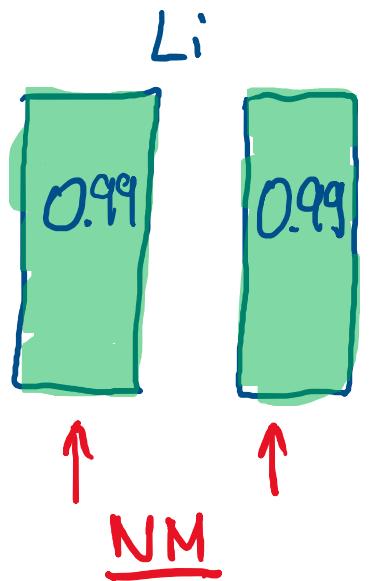
$$2NM \text{Ext}(\boxed{X}, \boxed{Y_1 \parallel Y_2}) = \boxed{\text{Li} \left( C(\boxed{X}, \boxed{Y_1}); \boxed{Y_2} \right)}$$



## A bit more history

Goyal, Srinivasan, Zhu '21 considered following

$$2NM \text{Ext}(\boxed{X}, \boxed{Y_1 \parallel Y_2}) = \text{Li} \left( C(\boxed{X}, \boxed{Y_1}); \boxed{Y_2} \right)$$



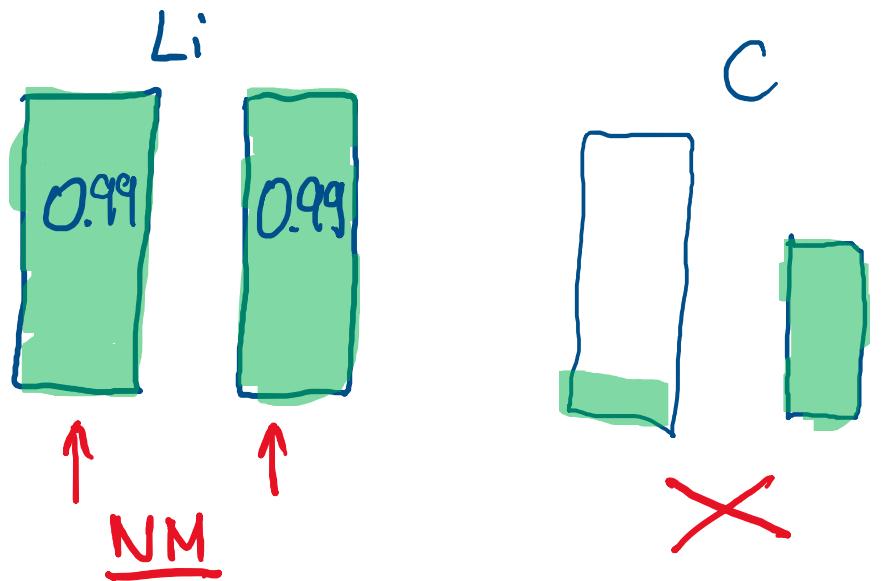
Problem

if  $y'_1 \neq y_1$   
 $x' \neq x$

## A bit more history

Goyal, Srinivasan, Zhu '21 considered following

$$2NM\text{Ext}(\boxed{X}, \boxed{Y_1 \parallel Y_2}) = \text{Li} \left( C(\boxed{X}, \boxed{Y_1}); \boxed{Y_2} \right)$$



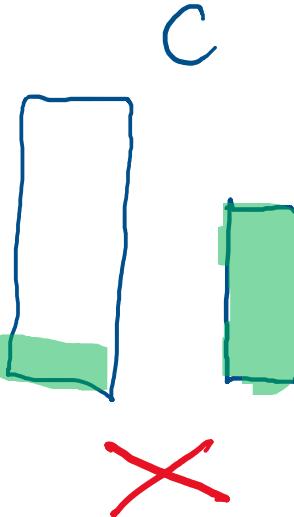
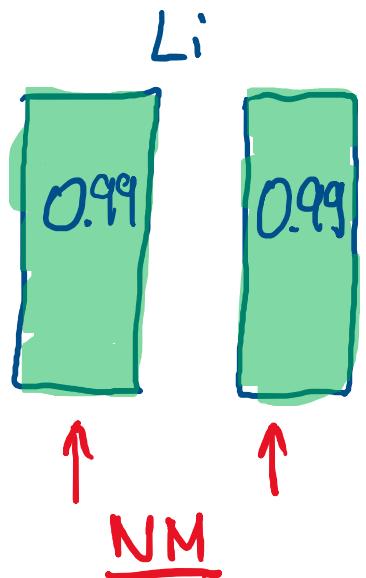
### Problem

if  $y'_1 \neq y_1$  but  $C(x', y'_1) = C(x, y_1)$   
 $x' \neq x$  then

## A bit more history

Goyal, Srinivasan, Zhu '21 considered following

$$2NM\text{Ext}(\boxed{X}, \boxed{Y_1 \parallel Y_2}) = \text{Li} \left( C(\boxed{X}, \boxed{Y_1}); \boxed{Y_2} \right)$$



### Problem

if  $\begin{matrix} Y'_1 \\ X' \end{matrix} \neq \begin{matrix} Y_1 \\ X \end{matrix}$  but  $C(X', Y'_1) = C(X, Y_1)$

then

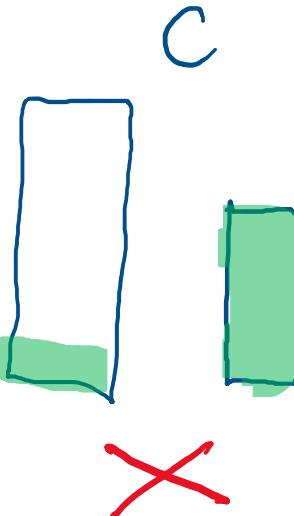
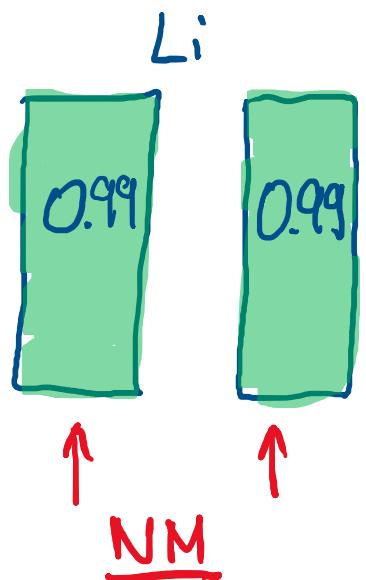
$$\text{Out}' = \text{Out.}$$

## A bit more history

Goyal, Srinivasan, Zhu '21 considered following

also has to be uniform since  $Li$  doesn't tolerate low entropy.

$$2NM \text{Ext}(\boxed{X}, \boxed{Y_1 \parallel Y_2}) = Li \left( C(\boxed{X}, \boxed{Y_1}); \boxed{Y_2} \right)$$



### Problem

if  $y'_1 \neq y_1$  but  $C(x', y'_1) = C(x, y_1)$   
 $x' \neq x$  then

$$\text{Out}' = \text{Out.}$$

# GSG transform with a twist(s)

Original

$$2NMEst(\boxed{X}, \boxed{Y_1 \parallel Y_2}) = Li \left( C(\boxed{X}, \boxed{Y_1}); \boxed{Y_2} \right)$$

# GSG transform with a twist(s)

Original

$$2\text{NME}_{\text{xt}}(\boxed{x}, \boxed{y_1 \parallel y_2}) = \text{Li} \left( C(\boxed{x}, \boxed{y_1}); \boxed{y_2} \right)$$

Twist

$$2\text{NME}_{\text{xt}}(\boxed{x}, \boxed{y_1 \parallel y_2}) = E \left( \quad \right)$$

# GSG transform with a twist(s)

Original

$$2\text{NME}_{\text{xt}}(\boxed{x}, \boxed{y_1 \parallel y_2}) = \text{Li} \left( C(\boxed{x}, \boxed{y_1}); \boxed{y_2} \right)$$

Twist

$$2\text{NME}_{\text{xt}}(\boxed{x}, \boxed{y_1 \parallel y_2}) = E \left( C(\boxed{x}, \boxed{y_1}), \quad \quad \quad \right)$$

# GSG transform with a twist(s)

Original

$$2NME_{\text{xt}}(\boxed{x}, \boxed{y_1 \parallel y_2}) = Li \left( C(\boxed{x}, \boxed{y_1}); \boxed{y_2} \right)$$

Twist

$$2NME_{\text{xt}}(\boxed{x}, \boxed{y_1 \parallel y_2}) = E \left( C(\boxed{x}, \boxed{y_1}), \boxed{y_1 \parallel y_2} \right)$$

# GSG transform with a twist(s)

Original

$$2\text{NME}_{\text{xt}}(\boxed{x}, \boxed{y_1 \parallel y_2}) = \text{Li} \left( C(\boxed{x}, \boxed{y_1}); \boxed{y_2} \right)$$

Twist

Problem  $C(x', y'_1) = C(x, y_1)$

$$2\text{NME}_{\text{xt}}(\boxed{x}, \boxed{y_1 \parallel y_2}) = E(C(\boxed{x}, \boxed{y_1}), \boxed{y_1 \parallel y_2})$$

# GSG transform with a twist(s)

Original

$$2\text{NME}_{\text{Ext}}(\boxed{x}, \boxed{y_1 \parallel y_2}) = \text{Li} \left( C(\boxed{x}, \boxed{y_1}); \boxed{y_2} \right)$$

Twist

Problem  $C(x', y'_1) = C(x, y_1)$

$$2\text{NME}_{\text{Ext}}(\boxed{x}, \boxed{y_1 \parallel y_2}) = E(C(\boxed{x}, \boxed{y_1}), \boxed{y_1 \parallel y_2})$$

if  $y'_1 \neq y_1$   $E$  will see it!

# GSG transform with a twist(s)

Original

$$2 \text{NME}_{\text{Ext}}(\boxed{x}, \boxed{y_1 \parallel y_2}) = \text{Li} \left( C(\boxed{x}, \boxed{y_1}); \boxed{y_2} \right)$$

Twist

Problem  $C(x', y'_1) = C(x, y_1)$

$$2 \text{NME}_{\text{Ext}}(\boxed{x}, \boxed{y_1 \parallel y_2}) = E(C(\boxed{x}, \boxed{y_1}), \boxed{y_1 \parallel y_2})$$

Problem

$$C(x', y'_1) = C(x, y_1)$$

# G1S2 transform with a twist(s)

Original

$$2\text{NME}_{\text{Ext}}(\boxed{x}, \boxed{y_1 \parallel y_2}) = \text{Li}\left(C(\boxed{x}, \boxed{y_1}); \boxed{y_2}\right)$$

Twist

Problem  $C(x', y'_1) = C(x, y_1)$

$$2\text{NME}_{\text{Ext}}(\boxed{x}, \boxed{y_1 \parallel y_2}) = E\left(C(\boxed{x}, \boxed{y_1}), \boxed{y_1 \parallel y_2}\right)$$

Problem

$$C(x', y'_1) = C(x, y_1)$$

All we need is ~~to~~ Collision Resistance

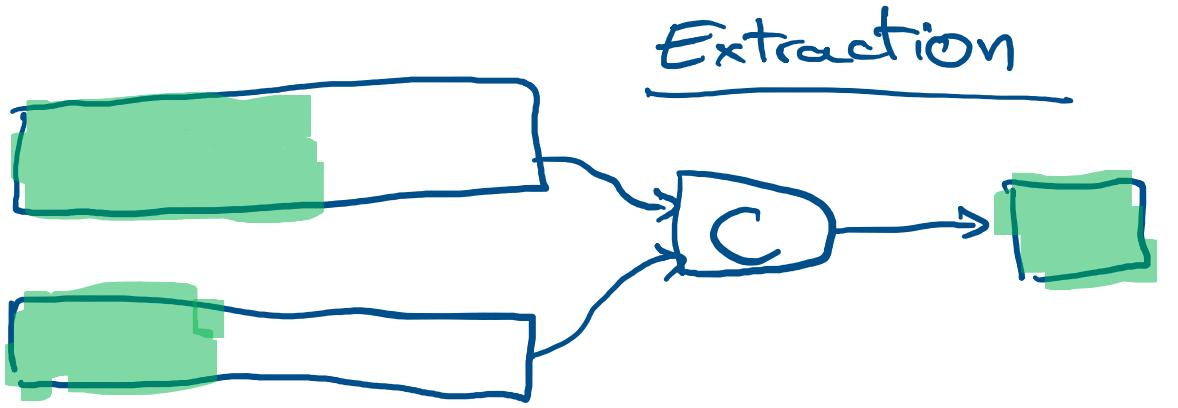
## Leftover hash Lemma

- if  $\Pr_{Y \leftarrow \cdot} [C(x_0, Y) = C(x_1, Y)]$  is tiny for all  $x_0 \neq x_1$   
then  $C$  is a good Extractor!

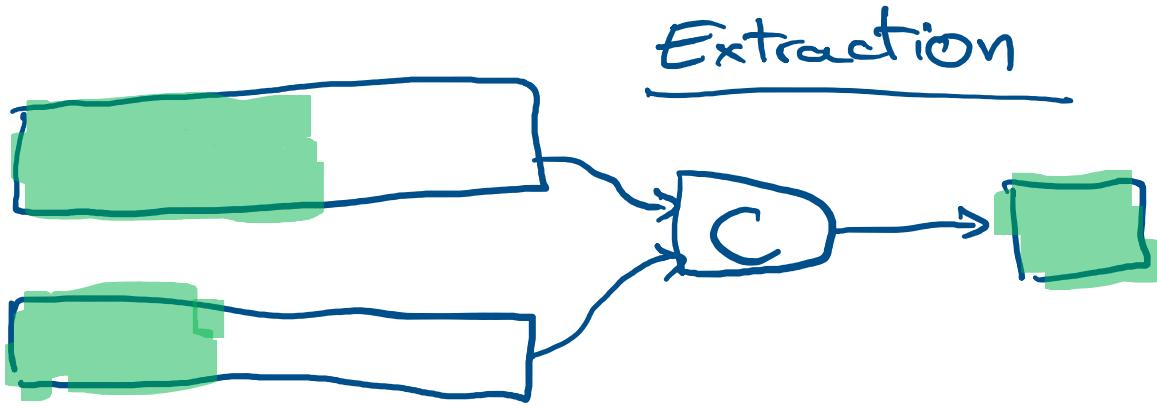
## Leftover hash Lemma

- if  $\Pr_{Y \leftarrow \cdot} [C(x_0, Y) = C(x_1, Y)]$  is tiny for all  $x_0 \neq x_1$   
then  $C$  is a good Extractor!
- In fact in [OS'18] we showed inverse is almost true too.

# Collision Resilient Extractors.



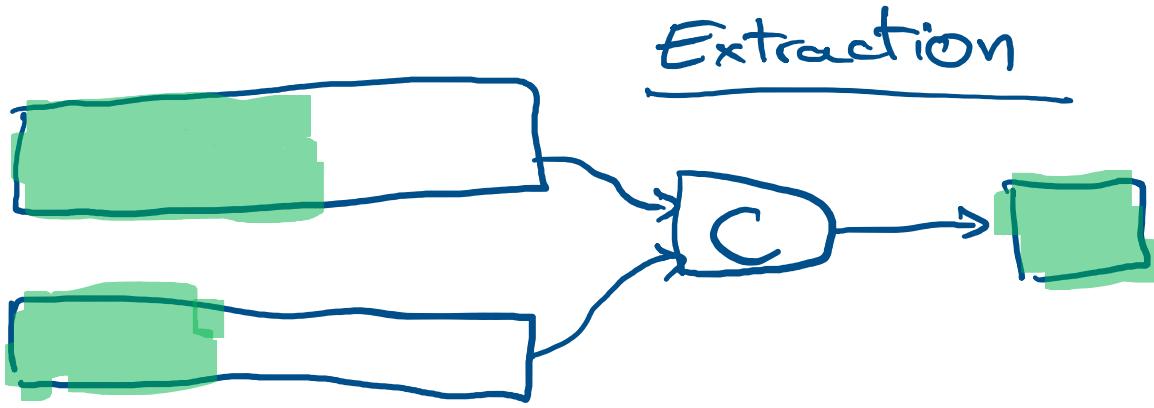
# Collision Resilient Extractors.



$$\underset{Y \leftarrow S}{\Pr} \left( C(X, Y) = C(X', Y) \right) \leq \text{tiny}$$

$X$  and  $X'$   
are arbitrarily  
correlated

# Collision Resilient Extractors.



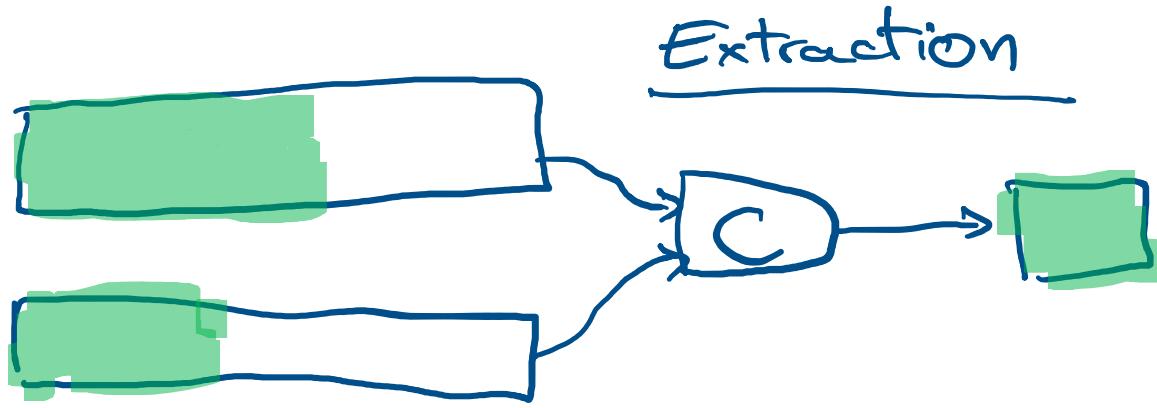
CR

$$P(C(x, y) = C(x', y)) \leq \text{tiny}$$

$x$  makes  
it even  
easier.

$x$  and  $x'$   
are arbitrarily  
correlated

# Collision Resilient Extractors.



CR

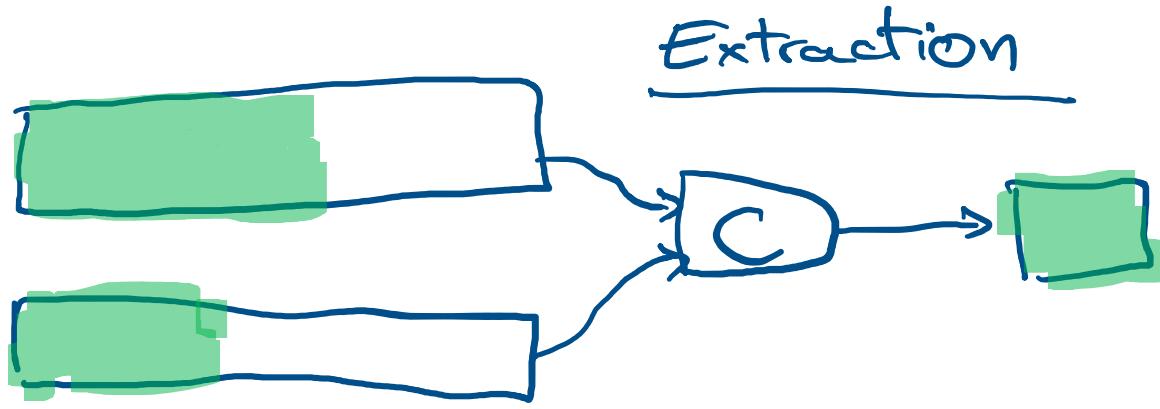
$$P(C(x, y) = C(x', y)) \leq \text{tiny}$$

$x$   
makes  
it even  
easier.

$x$  and  $x'$   
are arbitrarily  
correlated

What is CR :

# Collision Resilient Extractors.



CR

$$P(C(x, y) = C(x', y)) \leq \text{tiny}$$

$y \leftarrow s$

$x$

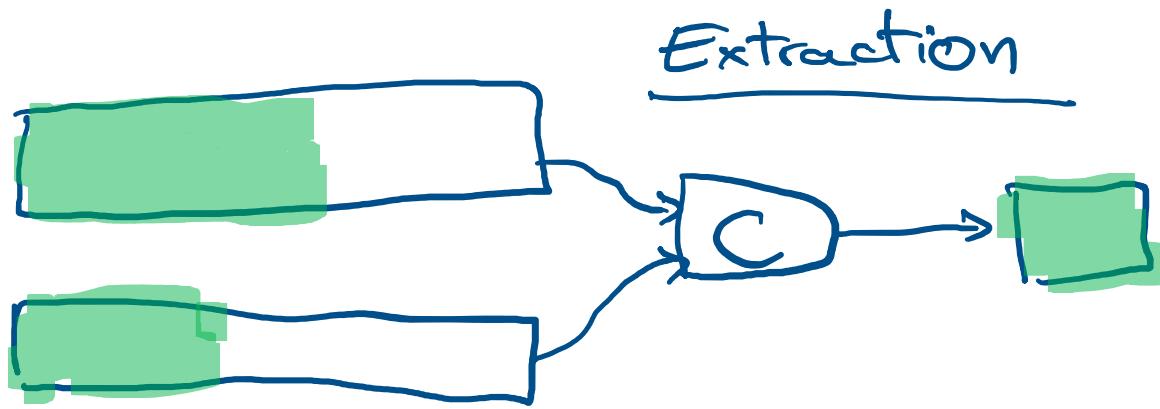
makes it even easier.

What is CR :

- Seeded Ext (can be compiled)



# Collision Resilient Extractors.



CR

$$P(C(x, y) = C(x', y)) \leq \text{tiny}$$

$y \leftarrow s$

$x$

makes it even easier.

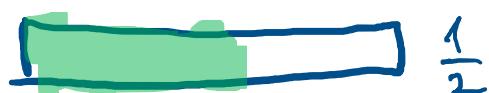
$x$  and  $x'$   
are arbitrarily correlated

## What is CR:

- Seeded Ext (can be compiled)



- Raz



## Construction

$$\underline{\text{FNME}}_x + \left( \boxed{x}, \boxed{Y_1 \amalg Y_2} \right) = \underline{\text{Li}} \left( \underline{\text{Te}} \left( \boxed{x}, \boxed{Y_1} \right), \boxed{Y_1 \amalg Y_2} \right)$$

## Construction

$$\underline{\text{FNME}}_x + \left( \boxed{x}, \boxed{Y_1 \amalg Y_2} \right) = \underline{\text{Li}} \left( \underline{\text{Te}} \left( \boxed{x}, \boxed{Y_1} \right), \boxed{Y_1 \amalg Y_2} \right)$$

## Construction

$$\underline{\text{FNME}}_x \left( \boxed{x}, \boxed{Y_1 \parallel Y_2} \right) = \underline{\text{Li}} \left( \underline{\text{Te}} \left( \boxed{x}, \boxed{Y_1} \right), \boxed{Y_1 \parallel Y_2} \right)$$

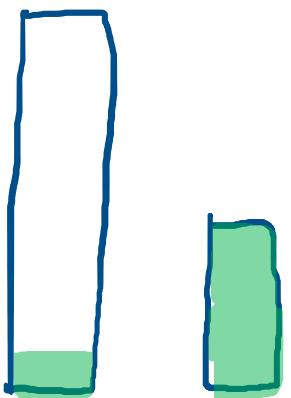
$\text{Te}$

The diagram illustrates the decomposition of the  $\text{Te}$  function. It shows two vertical bars: a blue bar labeled "polylog" and a green bar labeled "unif". Two arrows point from these bars towards the  $\text{Te}$  label above them, indicating that the  $\text{Te}$  function is composed of these two components.

## Construction

$$\underline{\text{FNME}_x} \left( \boxed{x}, \boxed{Y_1 \amalg Y_2} \right) = \underline{\text{Li}} \left( \underline{\text{Tre}} \left( \boxed{x}, \boxed{Y_1} \right), \boxed{Y_1 \amalg Y_2} \right)$$

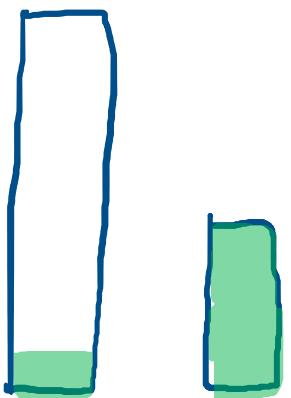
Tre



## Construction

$$\underline{\text{FNME}_x} \left( \boxed{x}, \boxed{Y_1 \amalg Y_2} \right) = \underline{\text{Li}} \left( \underline{\text{Tr}} \left( \boxed{x}, \boxed{Y_1} \right), \boxed{Y_1 \amalg Y_2} \right)$$

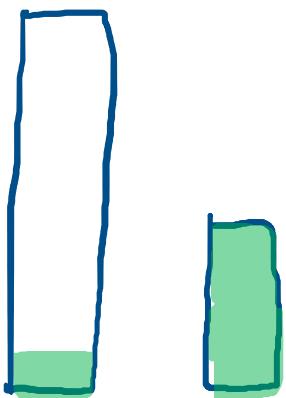
Tr



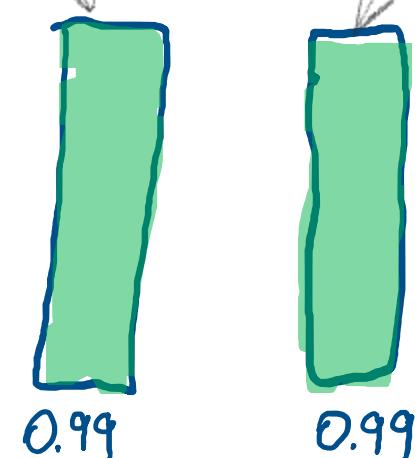
## Construction

$$\underline{\text{FNME}_x} \left( \boxed{x}, \boxed{Y_1 \amalg Y_2} \right) = \underline{\text{Li}} \left( \underline{\text{Te}} \left( \boxed{x}, \boxed{Y_1} \right), \boxed{Y_1 \amalg Y_2} \right)$$

Te



Li



## Construction

$$\underline{FNME_X}(X, Y_1 \parallel Y_2) = \underline{Li}(\underline{Tre}(X, Y_1), Y_1 \parallel Y_2)$$

gives Nonselectivity

gives low entropy of X.

$\underline{Tre}$

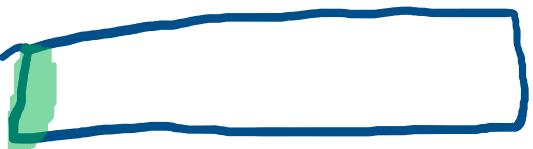
$\underline{Li}$

0.99

0.99

## Construction

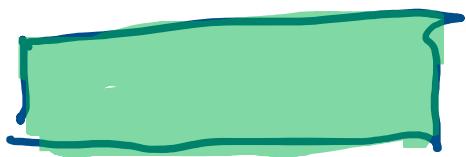
FNME<sub>x+</sub>



polylog



NM



uniform



## Construction

$$2NME_{xt}\left(\boxed{x}, \boxed{Y_1 \parallel Y_2}\right) = FNME_{xt}\left(Ray\left(\boxed{x}, \boxed{Y_1}\right), \boxed{Y_1 \parallel Y_2}\right)$$

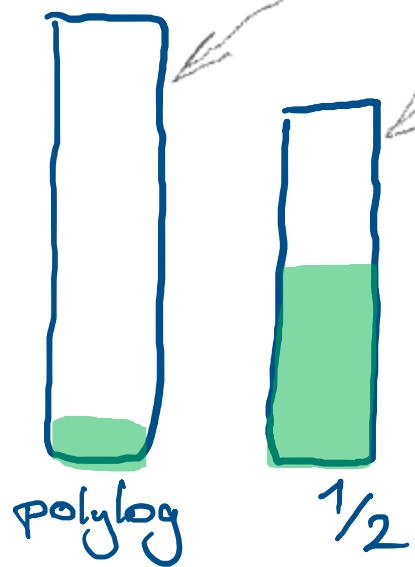
## Construction

$$2NME_{xt}\left(\boxed{x}, \boxed{y_1 \parallel y_2}\right) = FNME_{xt}\left(Ray\left(\boxed{x}, \boxed{y_1}\right), \boxed{y_1 \parallel y_2}\right)$$

# Construction

$$2\text{NME}_{\text{Ext}}\left(\boxed{x}, \boxed{Y_1 \parallel Y_2}\right) = \text{FNME}_{\text{Ext}}\left(\text{Raz}\left(\boxed{x}, \boxed{Y_1}\right), \boxed{Y_1 \parallel Y_2}\right)$$

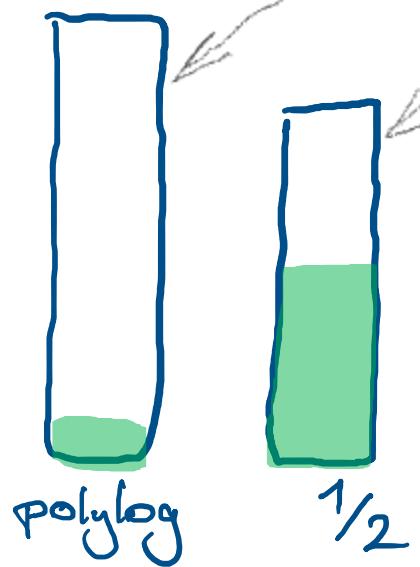
Raz



# Construction

$$2NME_{\text{Ext}}\left(\boxed{x}, \boxed{Y_1 \parallel Y_2}\right) = FNME_{\text{Ext}}\left(Raz\left(\boxed{x}, \boxed{Y_1}\right), \boxed{Y_1 \parallel Y_2}\right)$$

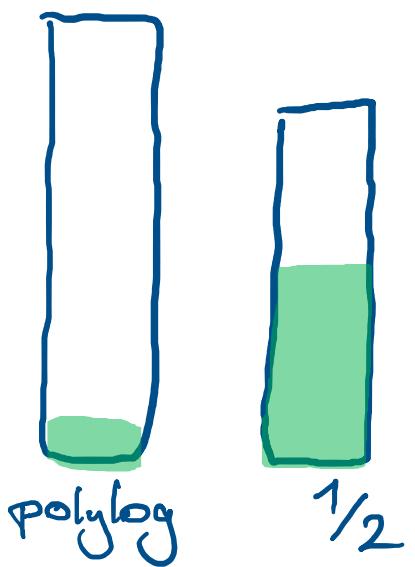
Raz



# Construction

$$2\text{NME}_{\text{Ext}}\left(\boxed{x}, \boxed{Y_1 \parallel Y_2}\right) = \text{FNME}_{\text{Ext}}\left(\text{Raz}\left(\boxed{x}, \boxed{Y_1}\right), \boxed{Y_1 \parallel Y_2}\right)$$

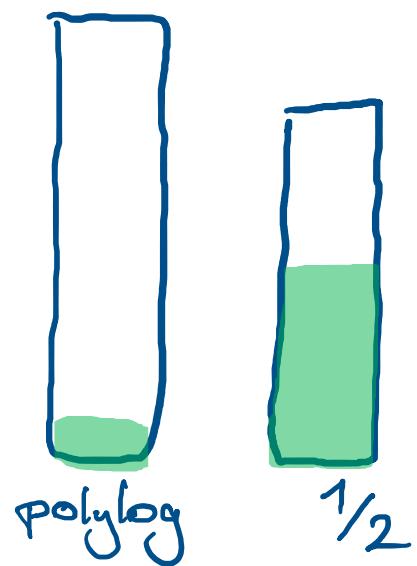
Raz



# Construction

$$2\text{NME}_{\text{Ext}}\left(\boxed{x}, \boxed{Y_1 \parallel Y_2}\right) = \text{FNM}_{\text{Ext}}\left(\text{Raz}\left(\boxed{x}, \boxed{Y_1}\right), \boxed{Y_1 \parallel Y_2}\right)$$

Raz

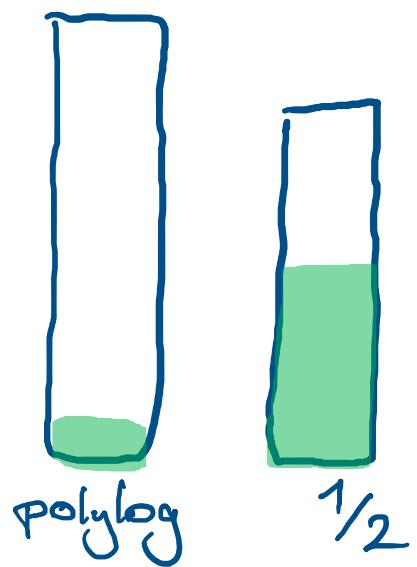


Entropy in  $Y_1$  has been used up so there is little left.

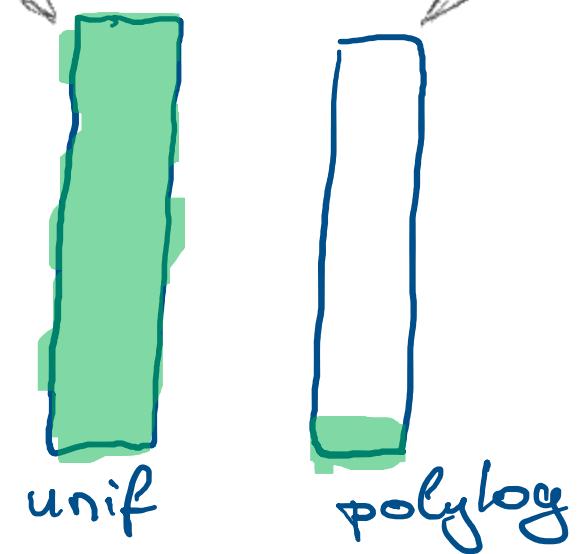
# Construction

$$2\text{NME}_{\text{Ext}}\left(\boxed{x}, \boxed{Y_1 \parallel Y_2}\right) = \text{FNME}_{\text{Ext}}\left(\text{Raz}\left(\boxed{x}, \boxed{Y_1}\right), \boxed{Y_1 \parallel Y_2}\right)$$

Raz



FNME<sub>ext</sub>

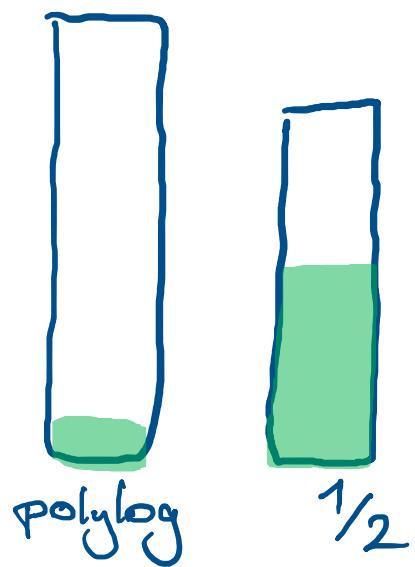


## Construction

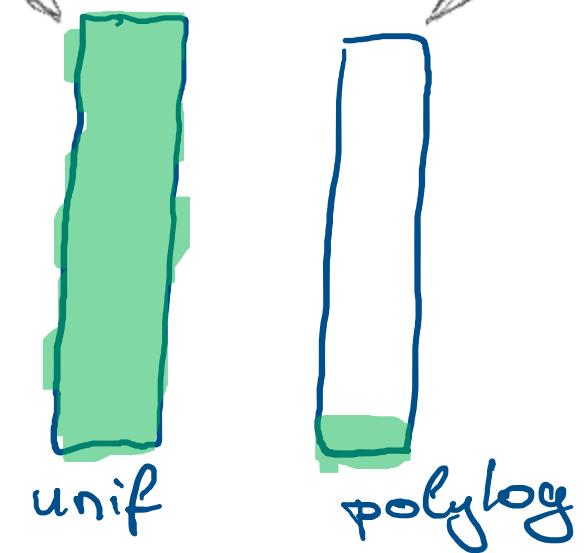
$$2\text{NME}_{\text{Ext}}\left(\boxed{x}, \boxed{Y_1 \parallel Y_2}\right) = \text{FNME}_{\text{Ext}}\left(\text{Raz}\left(\boxed{x}, \boxed{Y_1}\right), \boxed{Y_1 \parallel Y_2}\right)$$

gives Non-Malleability  
allows for lower entropies

Raz

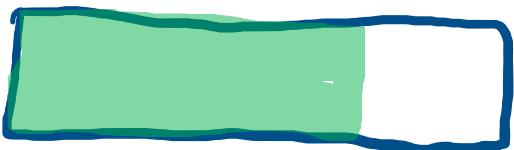


FNME<sub>ext</sub>



## Final Result

Full NM



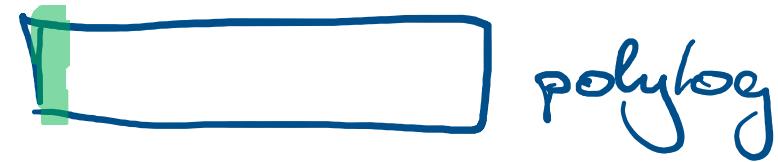
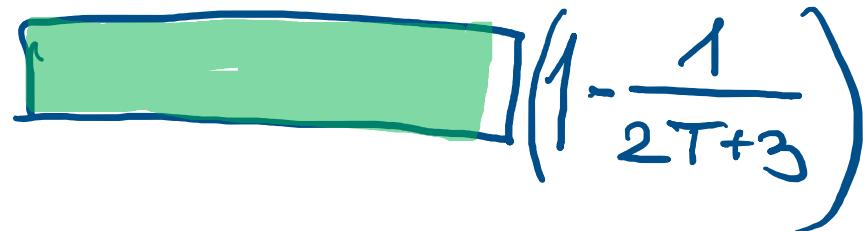
0.8

And



Polylog

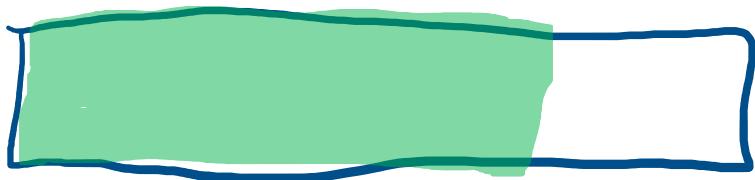
T-Multitamper NM



polylog

## Subsequent Work

Li:



$2/3$



polylog.

single tampering.

Why Care ?

# Why Care ?

2 NMExt are cool tools :

Privacy  
Amplification

Network  
Extraction

NMC

NM  
Secret  
Sharing

Leak Resi  
Tamper Resi

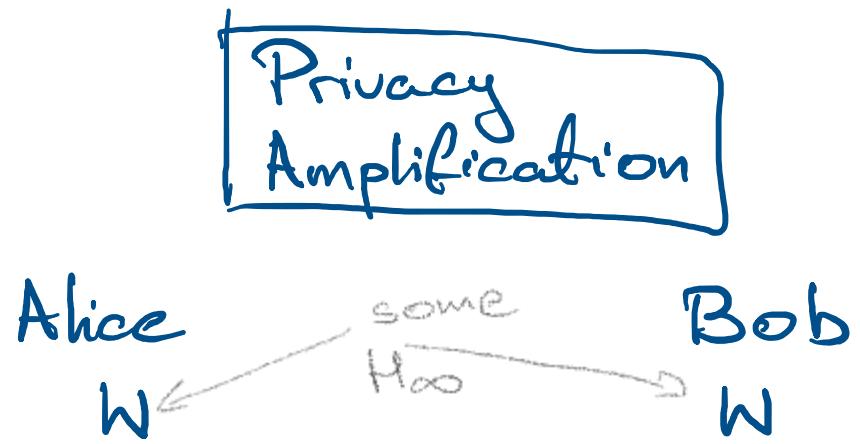
## Why Care ?

2 NME<sub>xt</sub> are cool tools :

Privacy  
Amplification

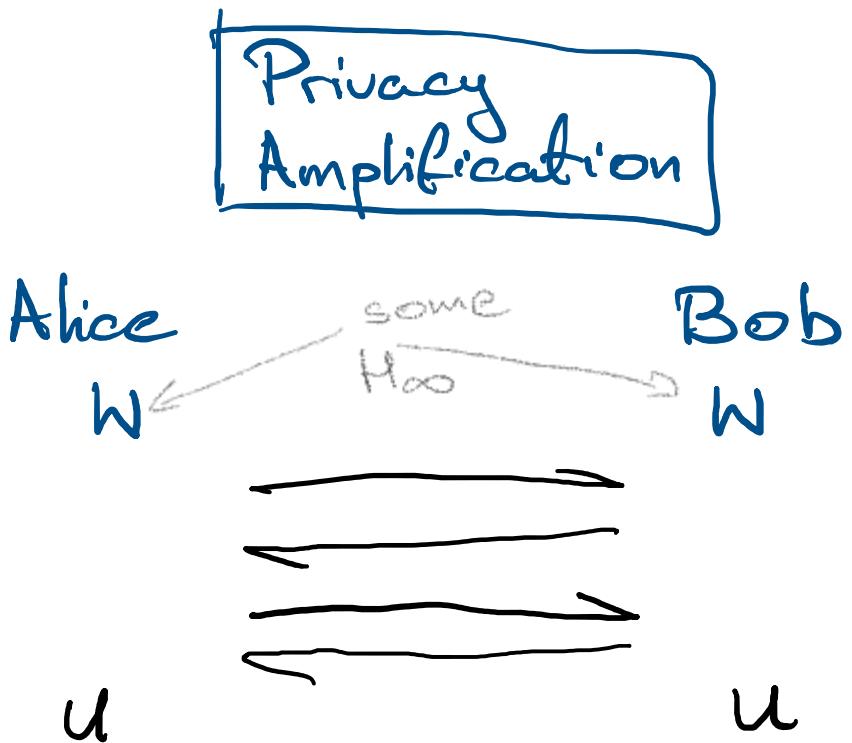
## Why Care ?

2 NME<sub>xt</sub> are cool tools :



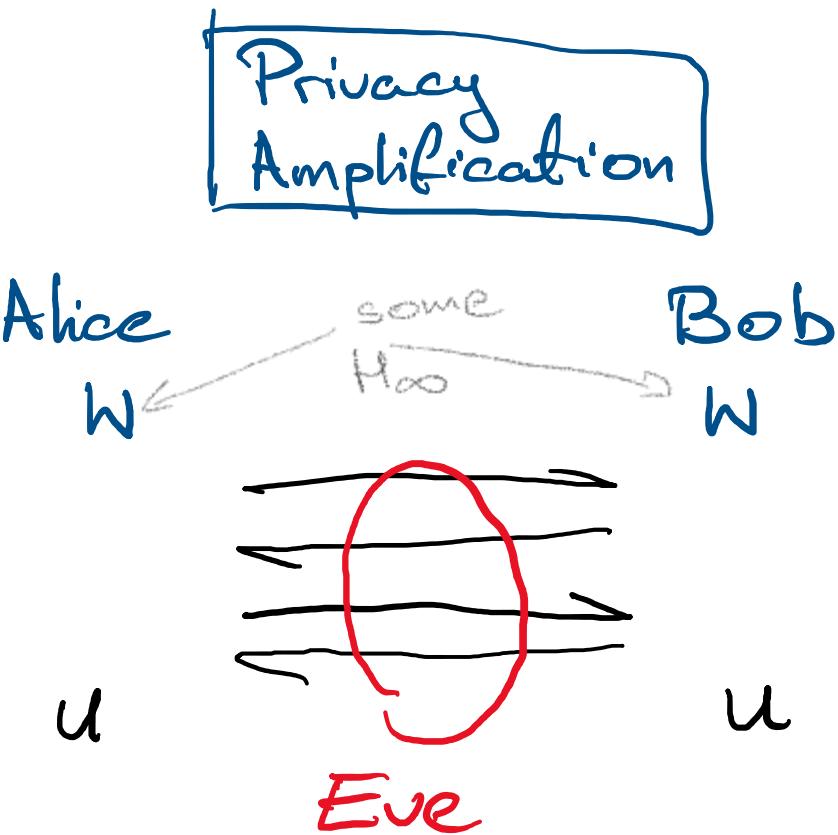
# Why Care ?

2 NME<sub>xt</sub> are cool tools :



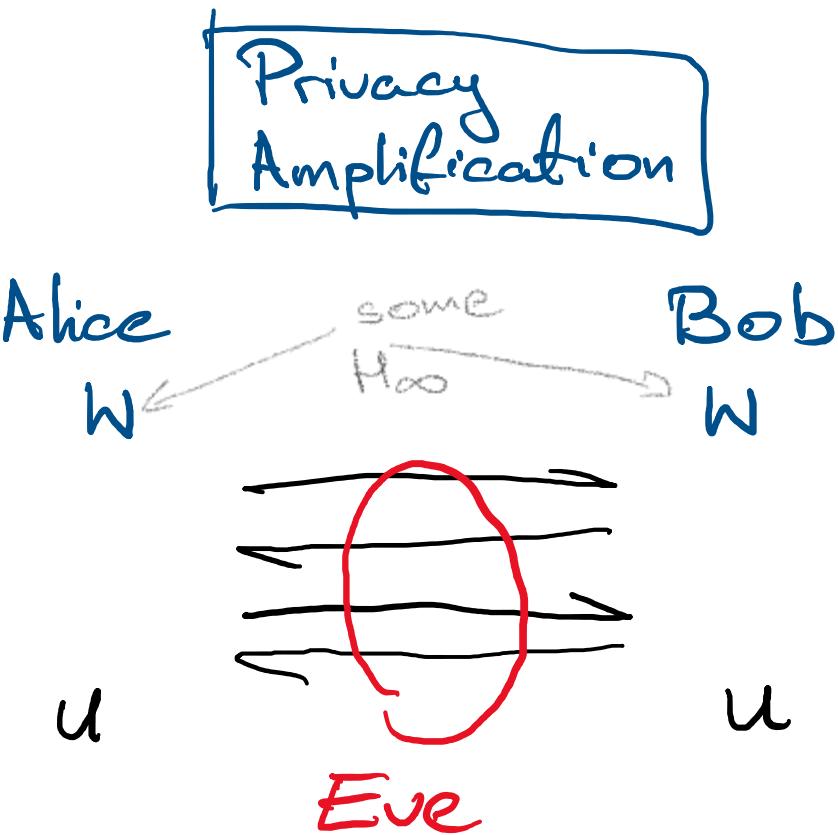
## Why Care ?

2 NME<sub>xt</sub> are cool tools :



# Why Care?

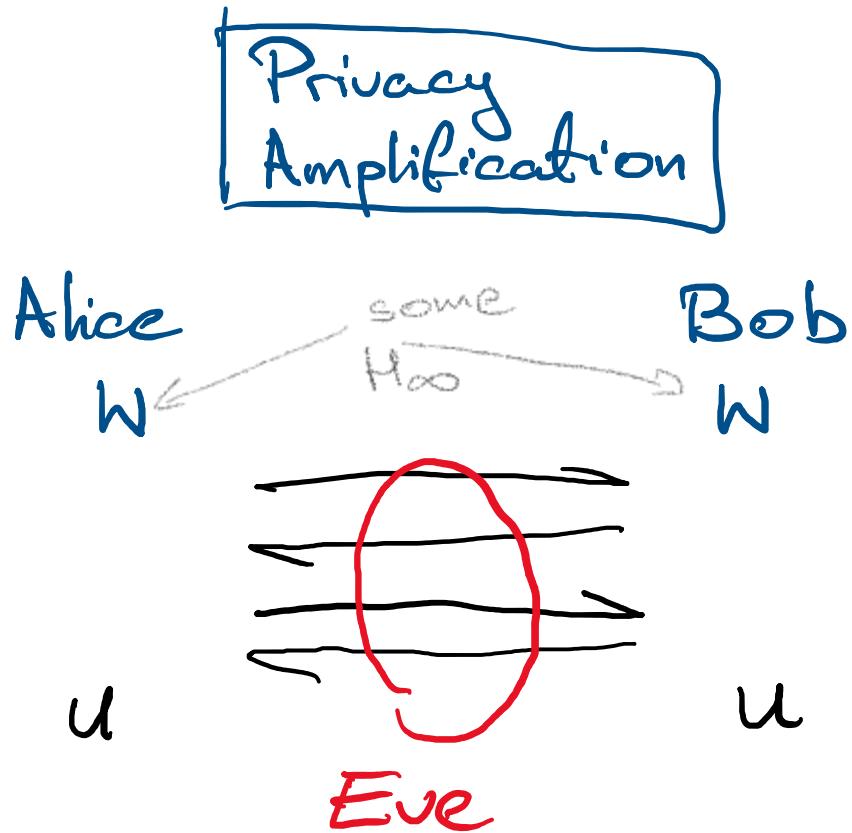
2 NME<sub>xt</sub> are cool tools:



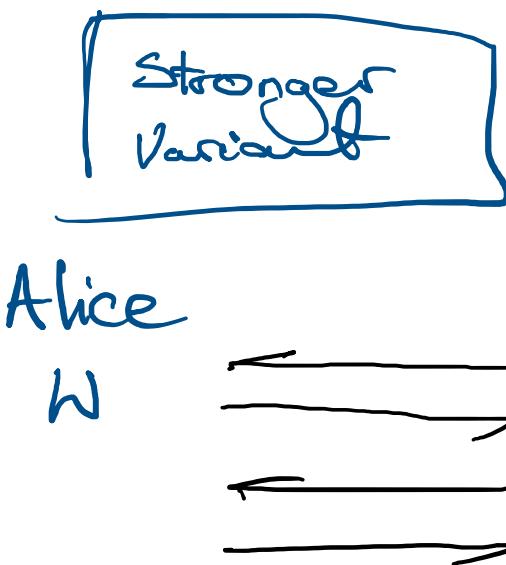
Seeded nMEx<sub>t</sub>

# Why Care?

2 NME<sub>xt</sub> are cool tools:

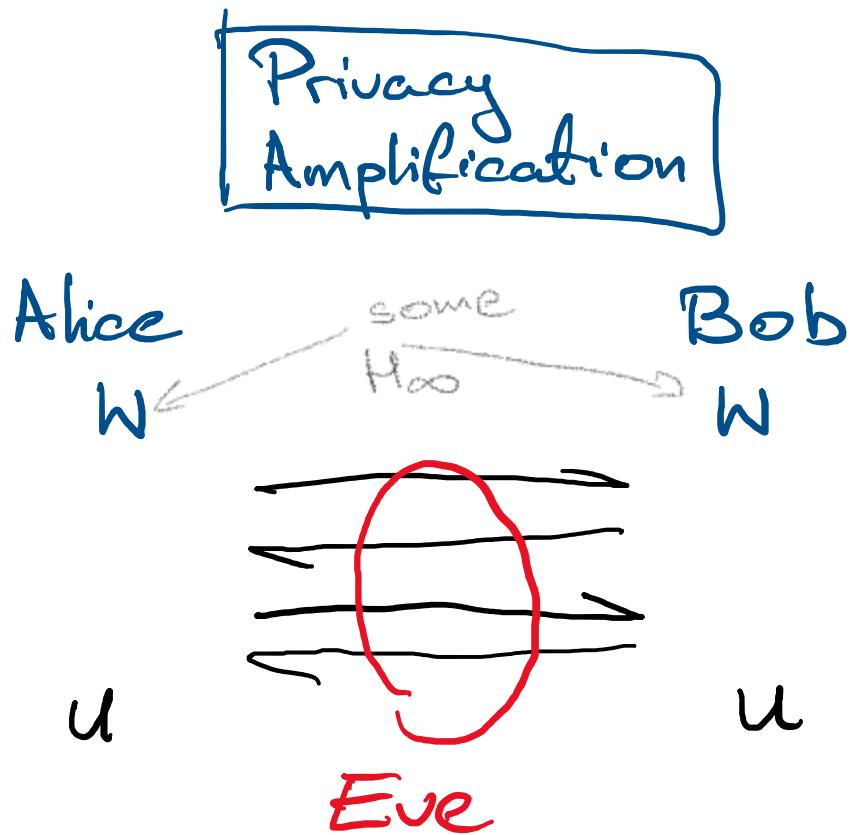


Seeded nMEx<sub>t</sub>

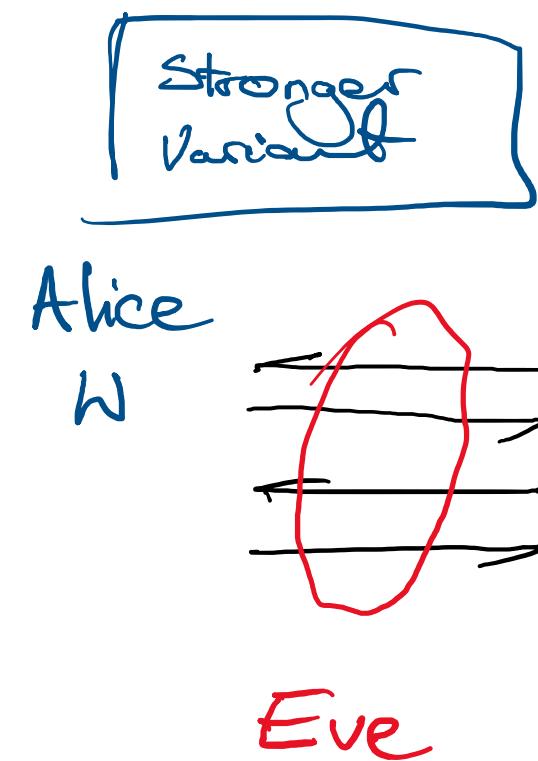


# Why Care?

2 NME<sub>xt</sub> are cool tools:



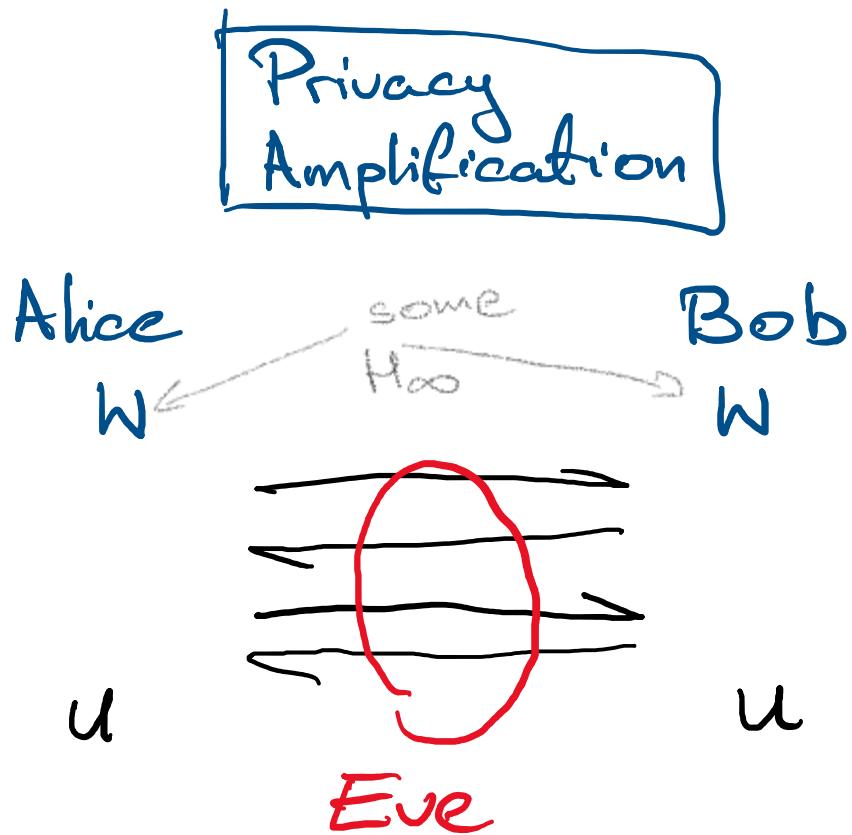
Seeded nMEx<sub>t</sub>



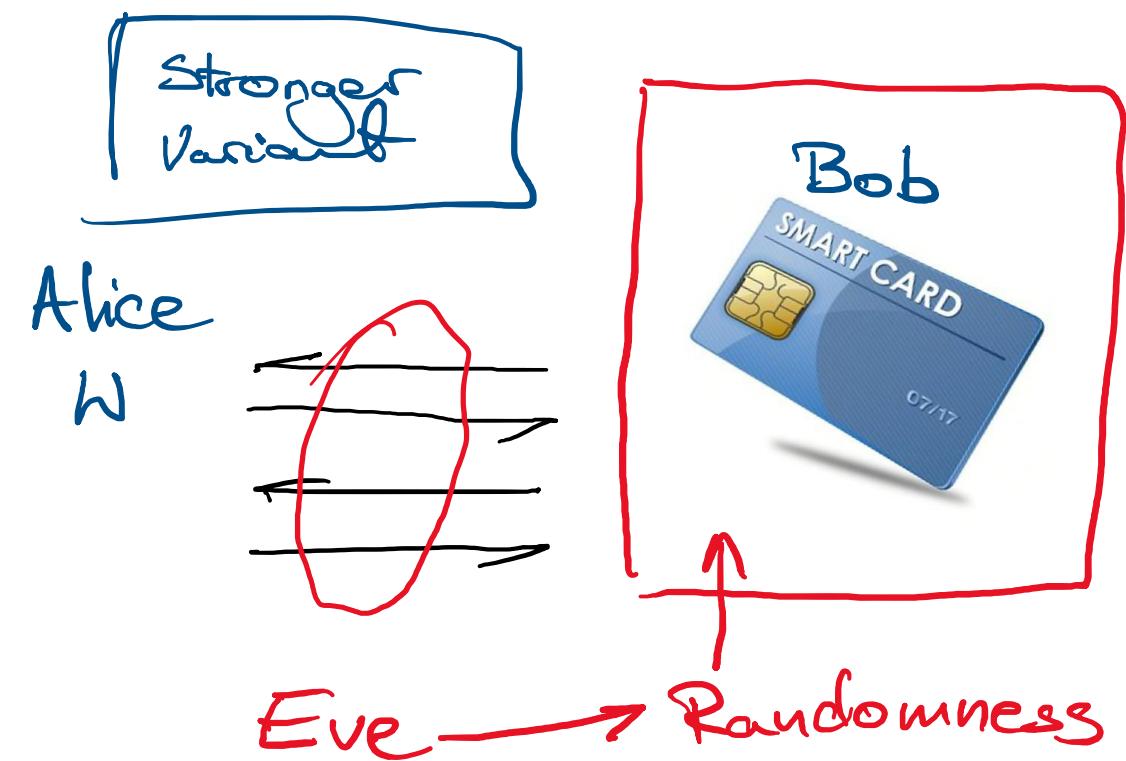
Bob

# Why Care?

2 NME<sub>xt</sub> are cool tools:

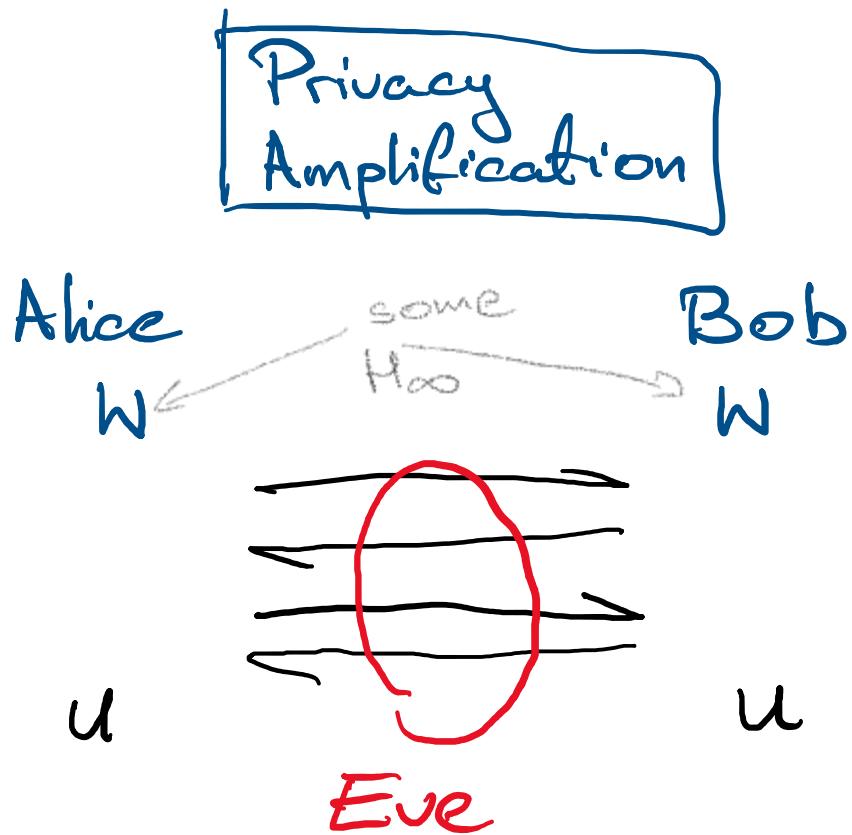


Seeded nMEx<sub>t</sub>

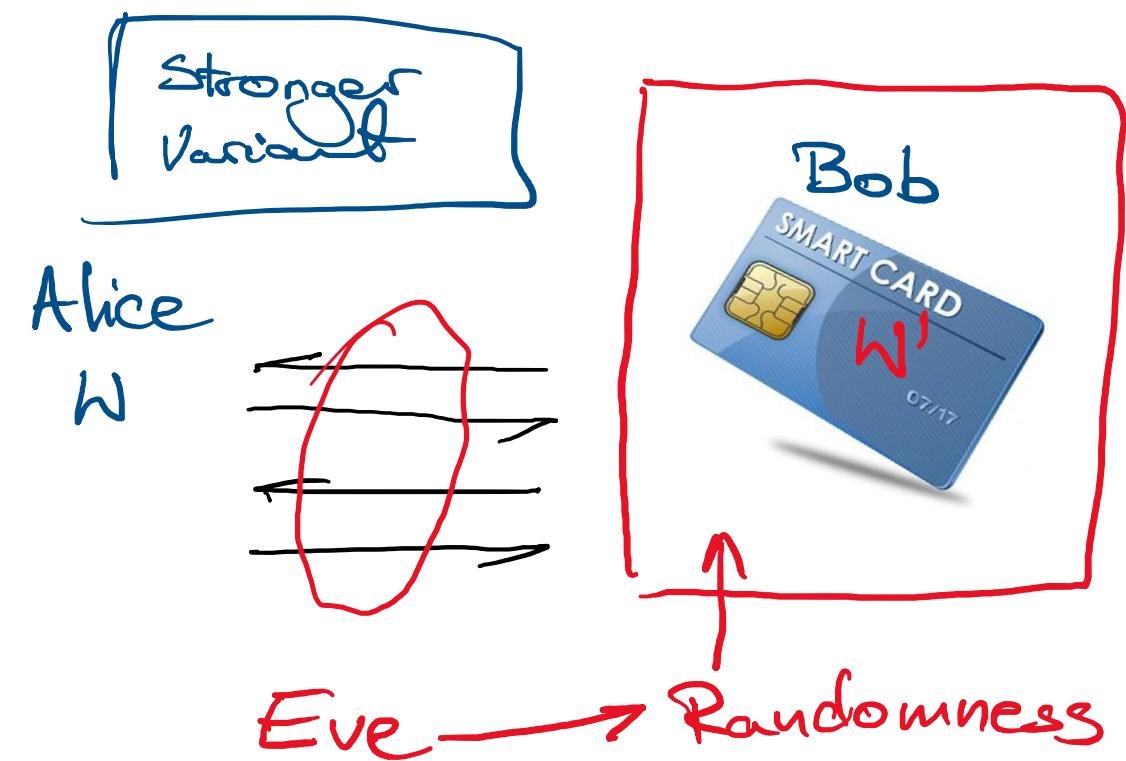


# Why Care?

2 NME<sub>xt</sub> are cool tools:

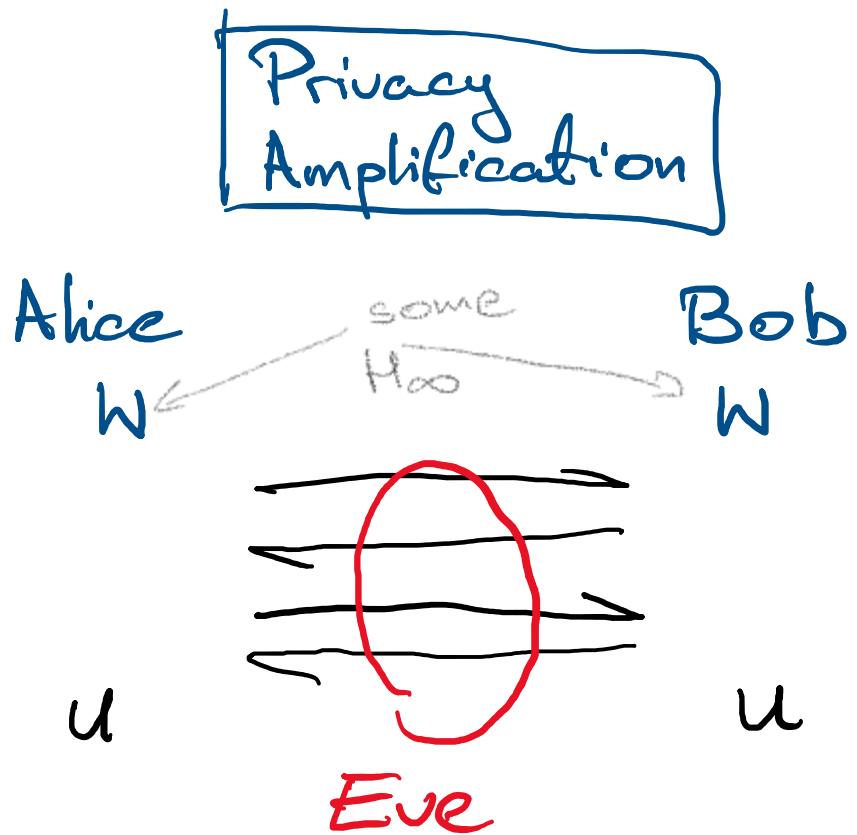


Seeded nMEx<sub>t</sub>

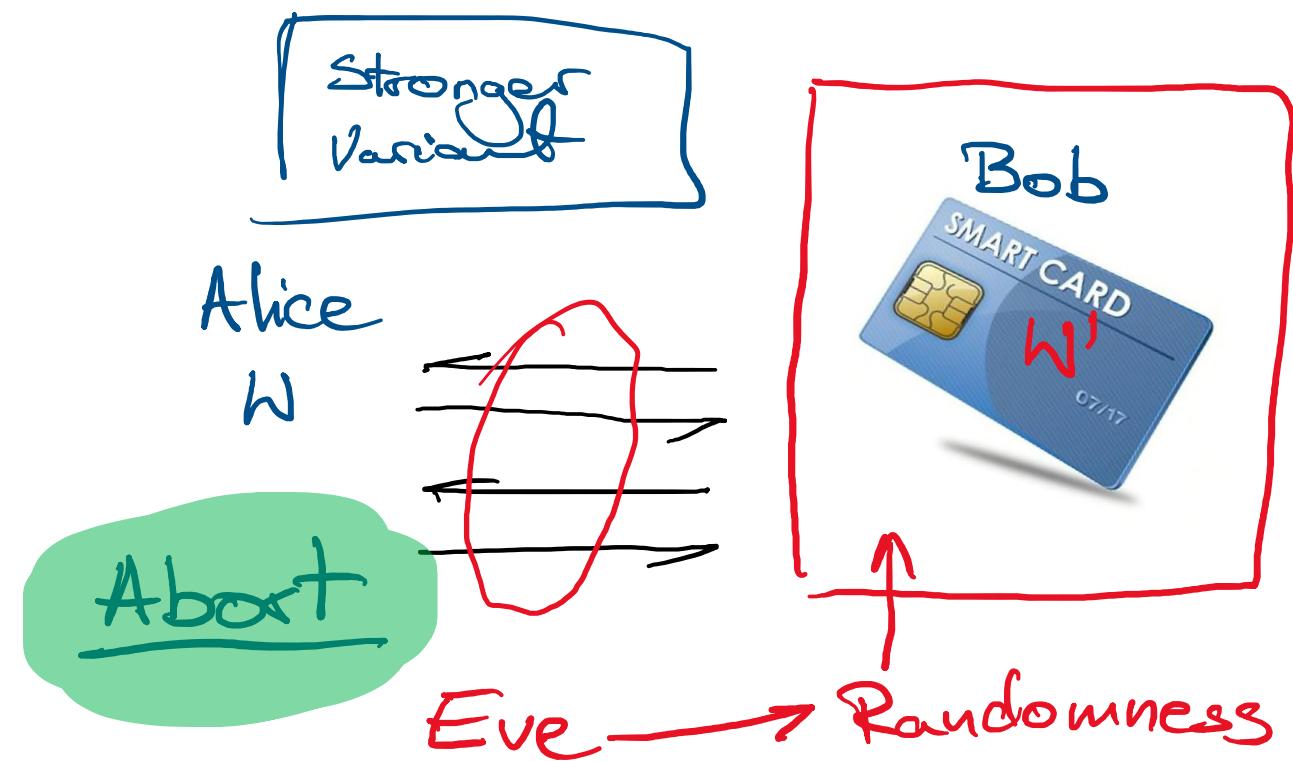


# Why Care?

2 NmExt are cool tools:



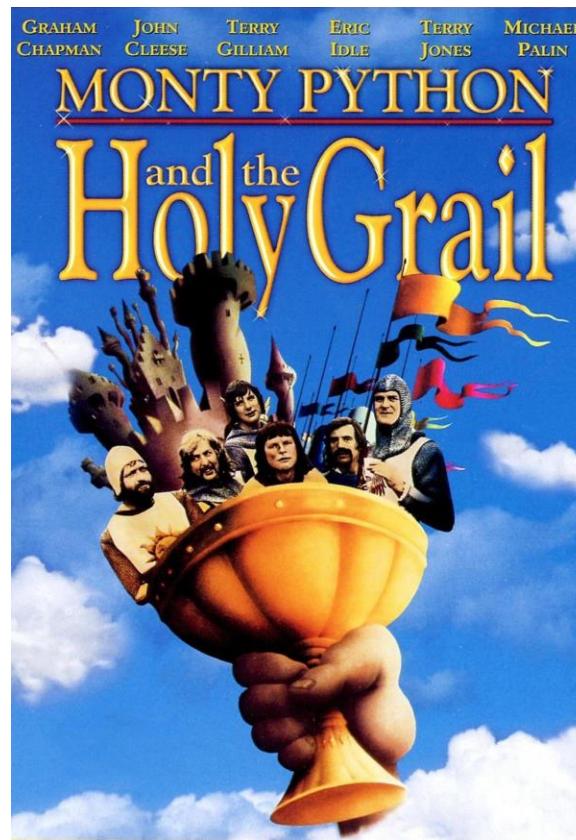
Seeded nmExt



2 nmExt.

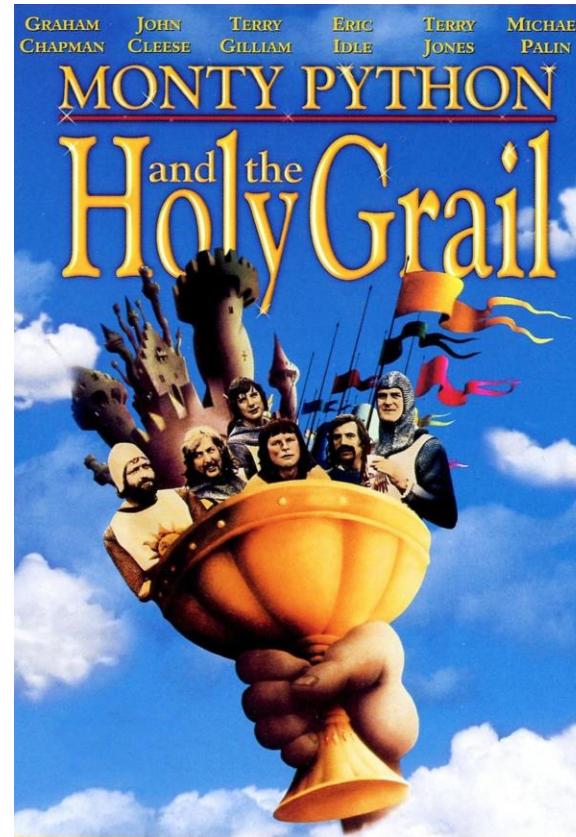
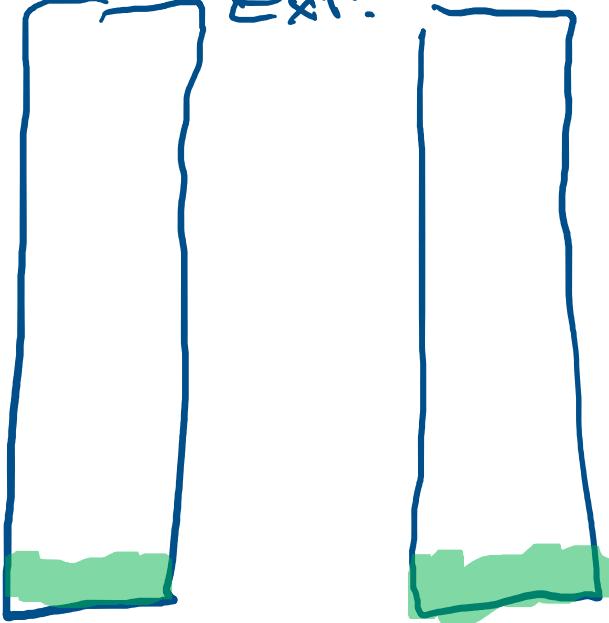
Why I care

Why I care



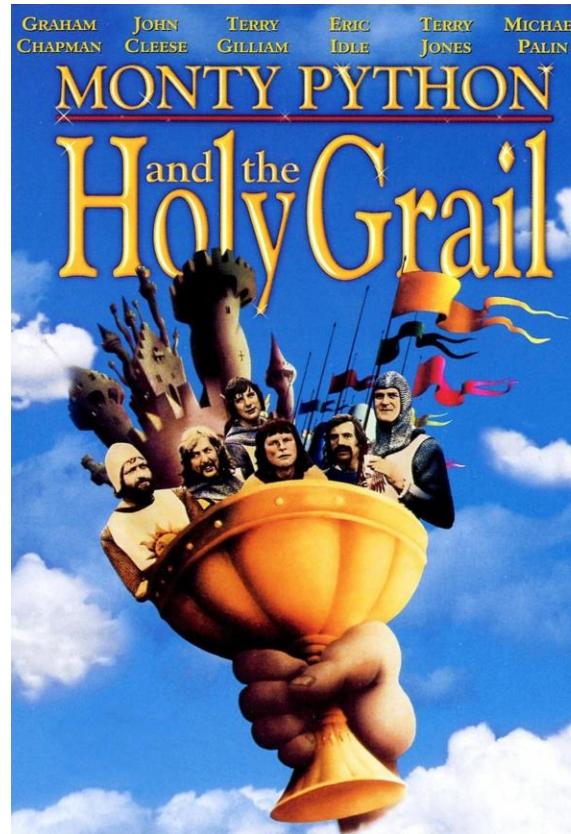
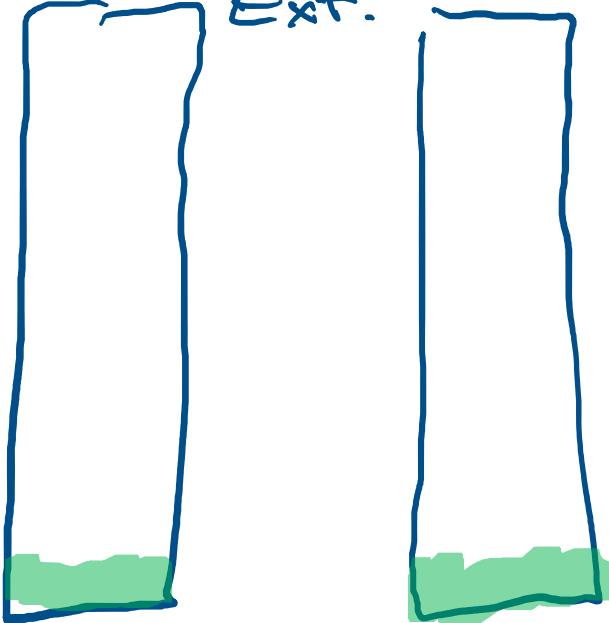
# Why I care

2 source  
Ext.



# Why I care

2 source  
Ext.



Entropy Rate

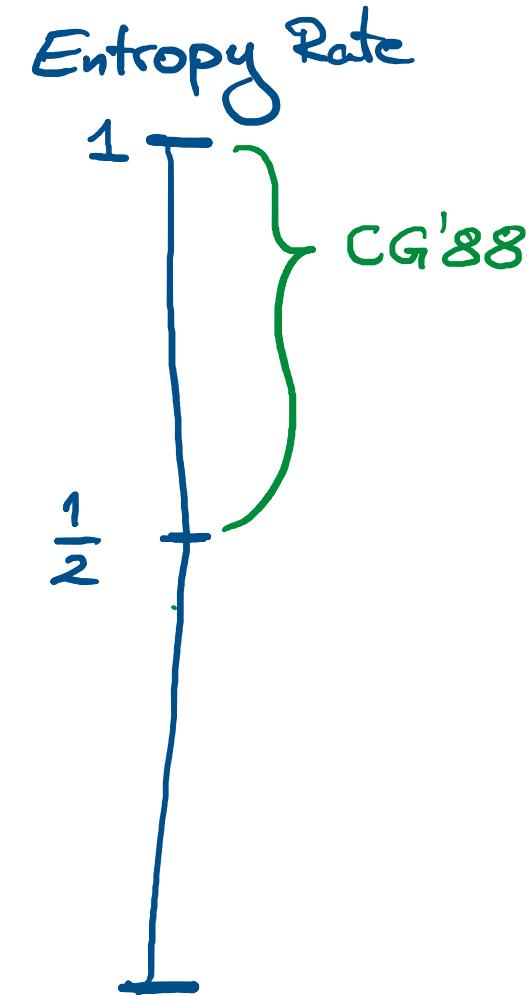
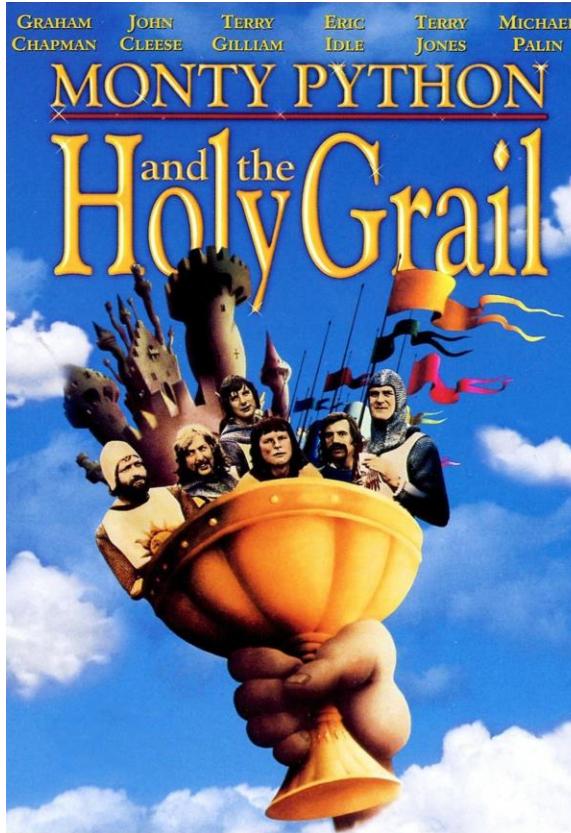
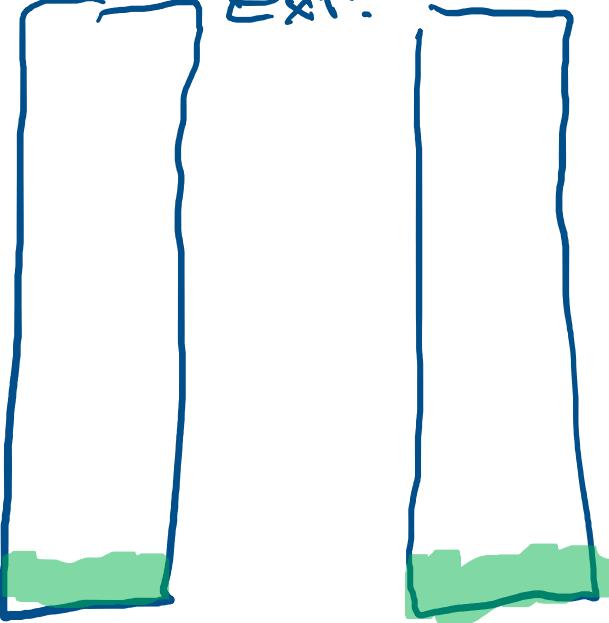
1

$\frac{1}{2}$



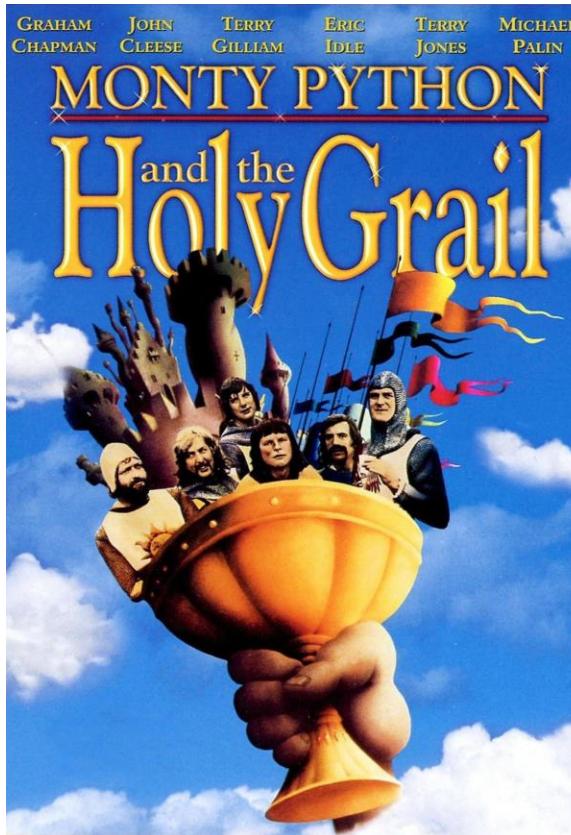
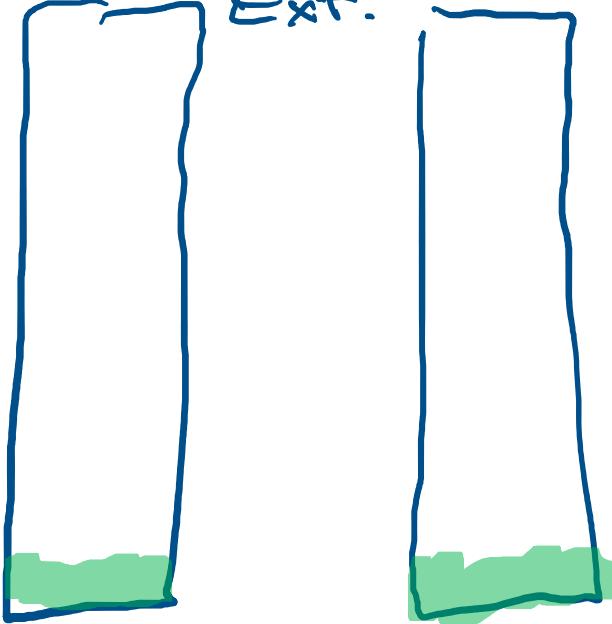
# Why I care

2 source  
Ext.



# Why I care

2 source  
Ext.



Entropy Rate

1

CG'88

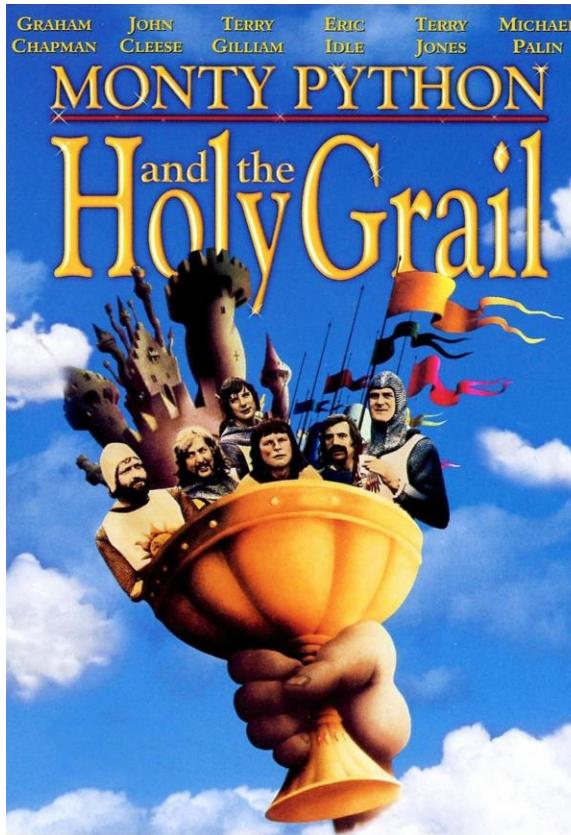
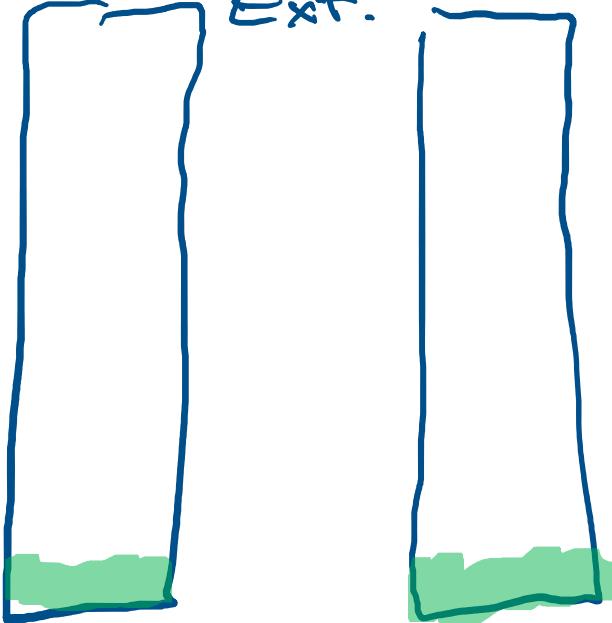
$\frac{1}{2}$

Bou'05

0

# Why I care

2 source  
Ext.



Entropy Rate

1

$\frac{1}{2}$

CG '88

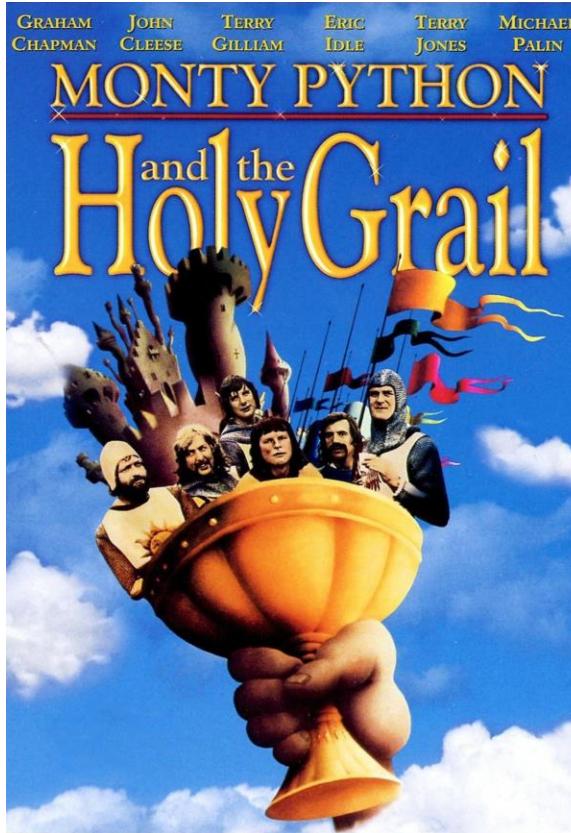
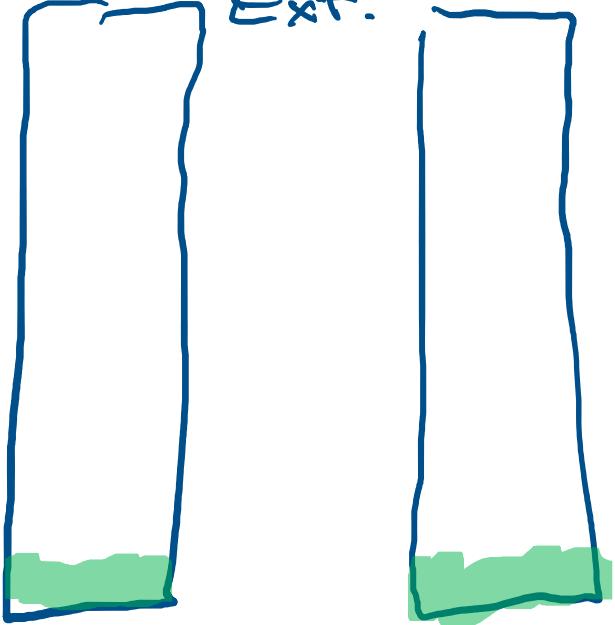
Bou '05

Lew '19

$\frac{4}{9}$

# Why I care

2 source  
Ext.



Entropy Rate

1

CG'88

$\frac{1}{2}$

Bou'05

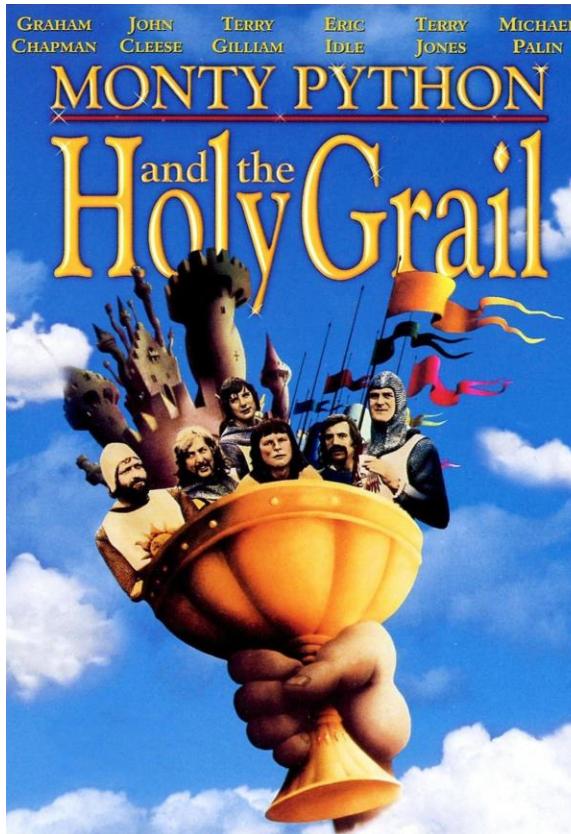
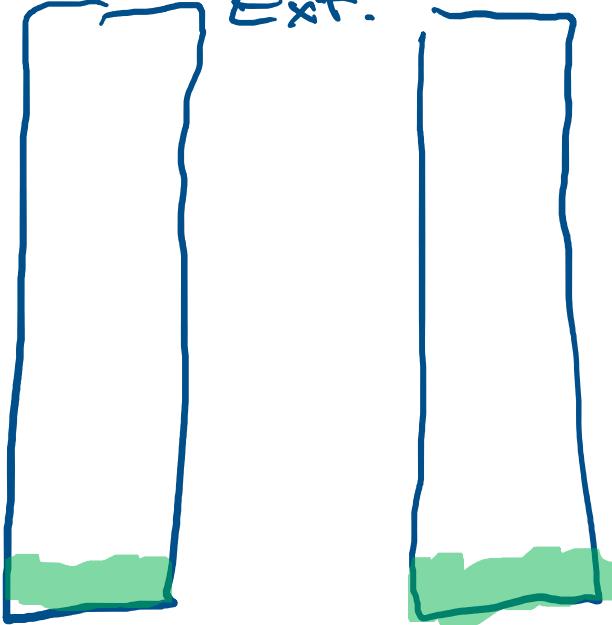
Lew'19

Cz'14

$\frac{1}{\log}$  poly error.

# Why I care

2 source  
Ext.



Entropy Rate

1

CG'88

$\frac{1}{2}$

Bou'05

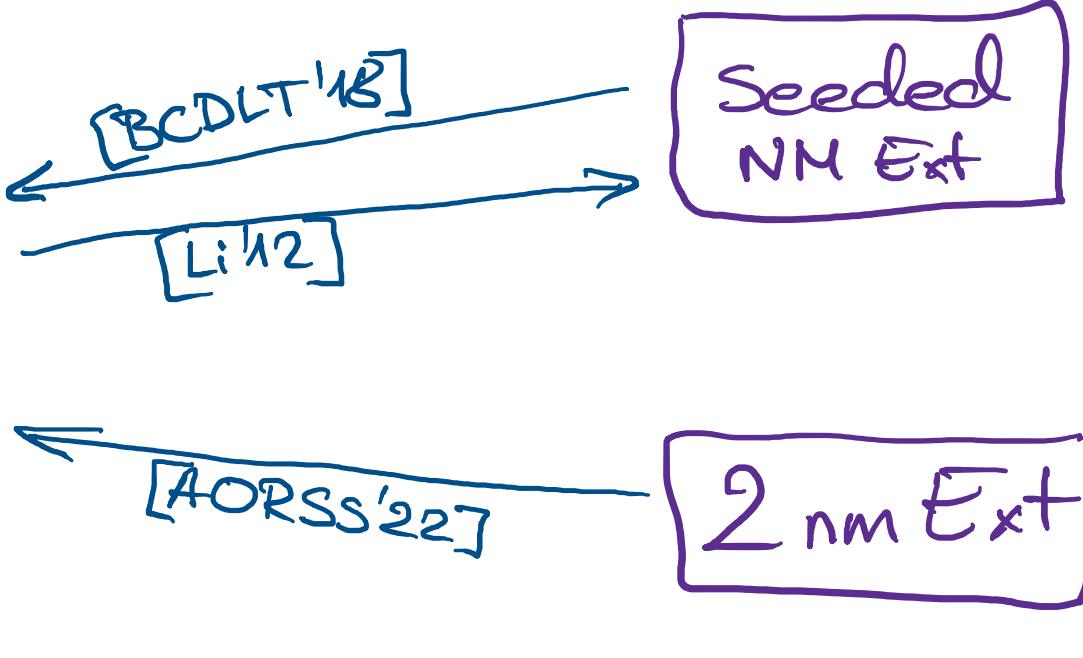
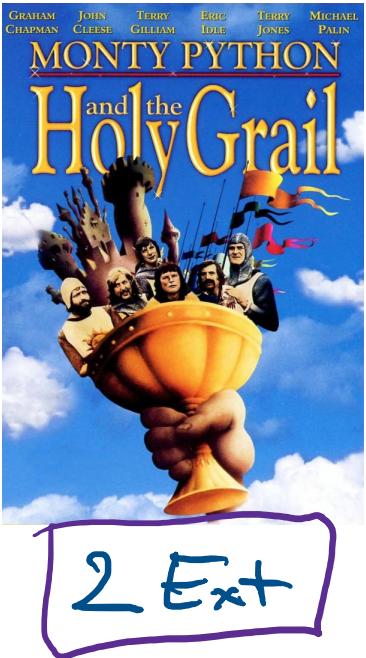
$\frac{4}{9}$

Lew'19

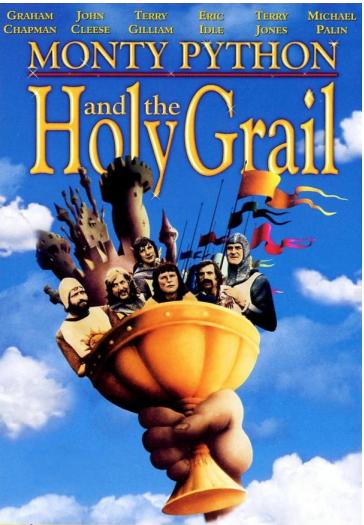
CZ'14

$\log$   
 $\frac{1}{\text{poly error.}}$

# Connections



# Connections



2 Ext

[BCDLT'18]  
[Li'12]

Seeded  
NM Ext

[AORSS'22]

2 nm Ext

$(1 - \frac{1}{T})$  entropy threshold

this paper gets  $(1 - \frac{1}{2T+3})$

Thank You

