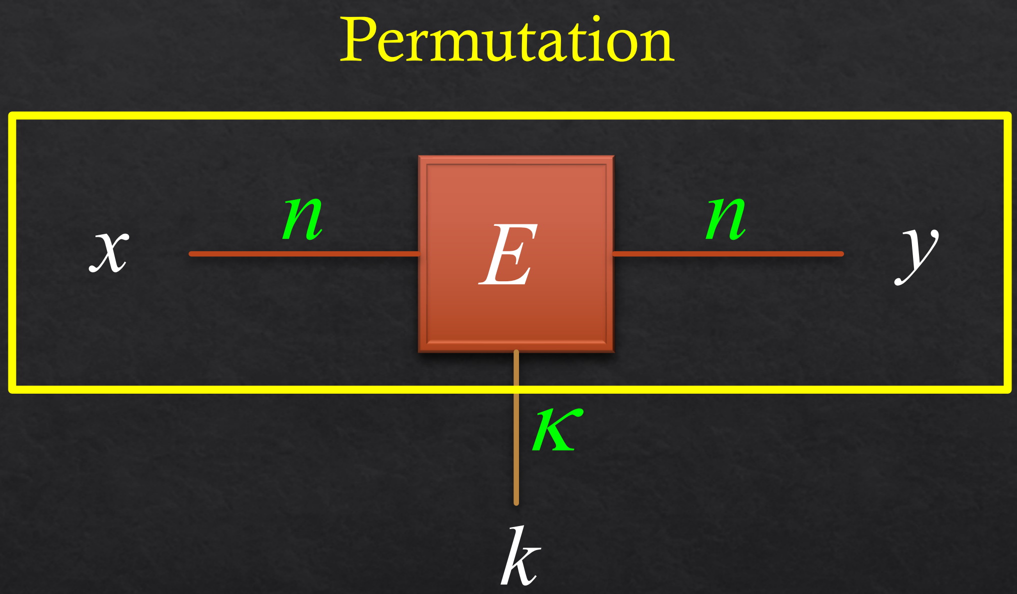
Tight Security Bounds for Key-Alternating Ciphers

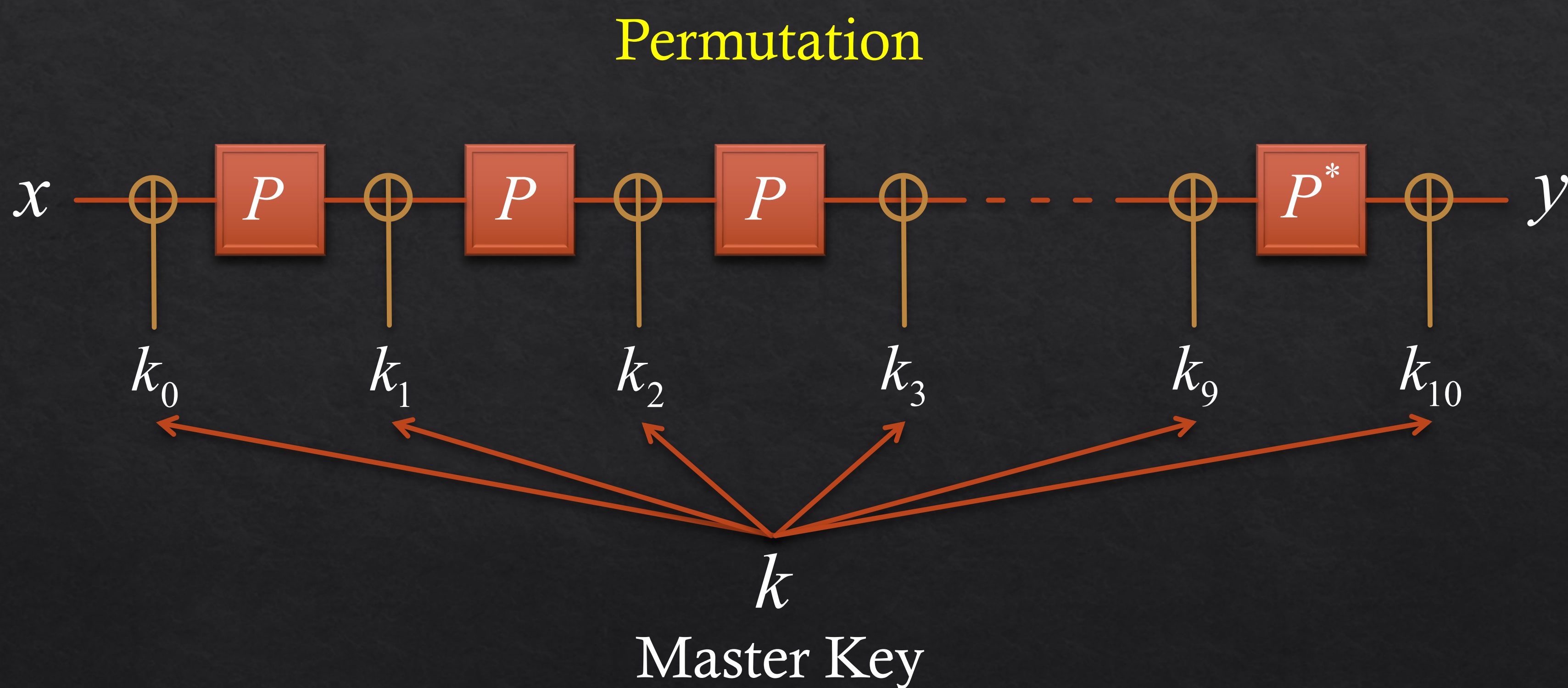
Shan Chen John Steinberger

IIIS, Tsinghua University

Block Cipher

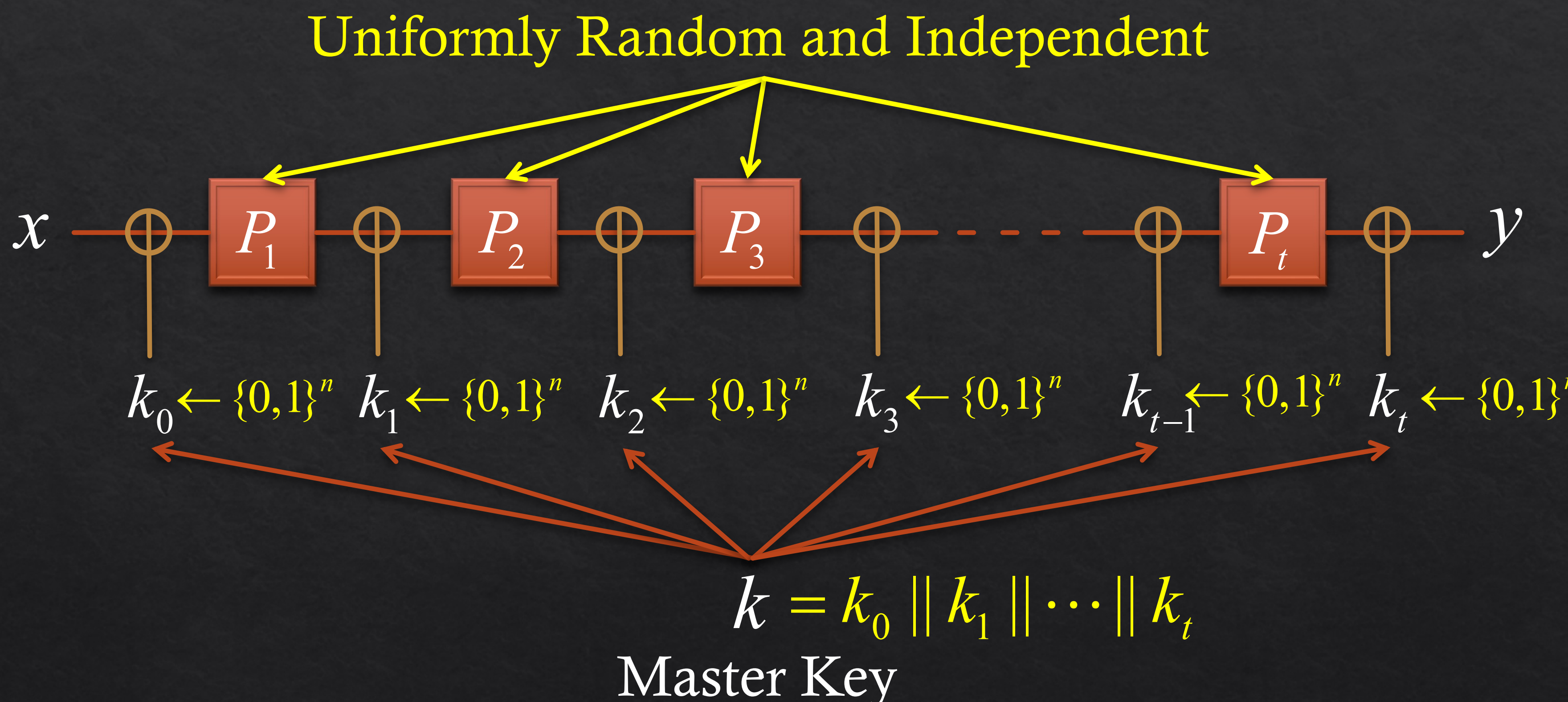


AES Cipher

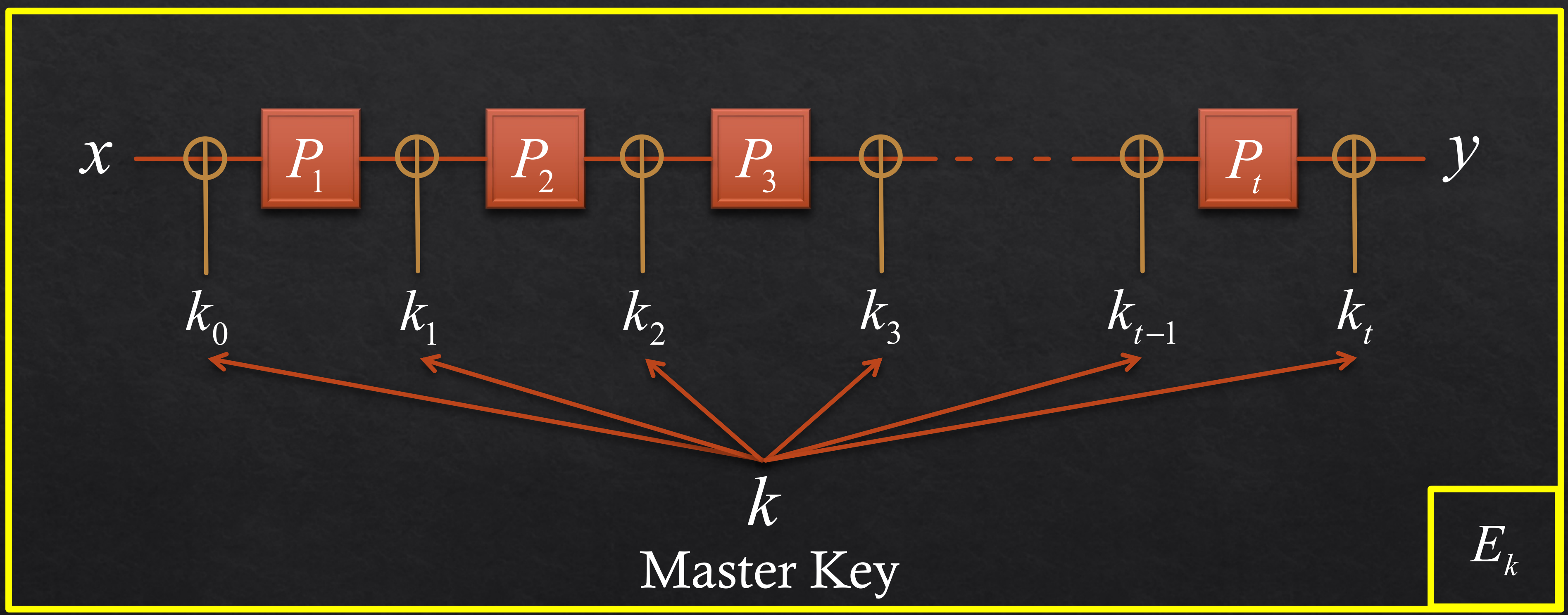


$\approx_C$ Random Permutation Q

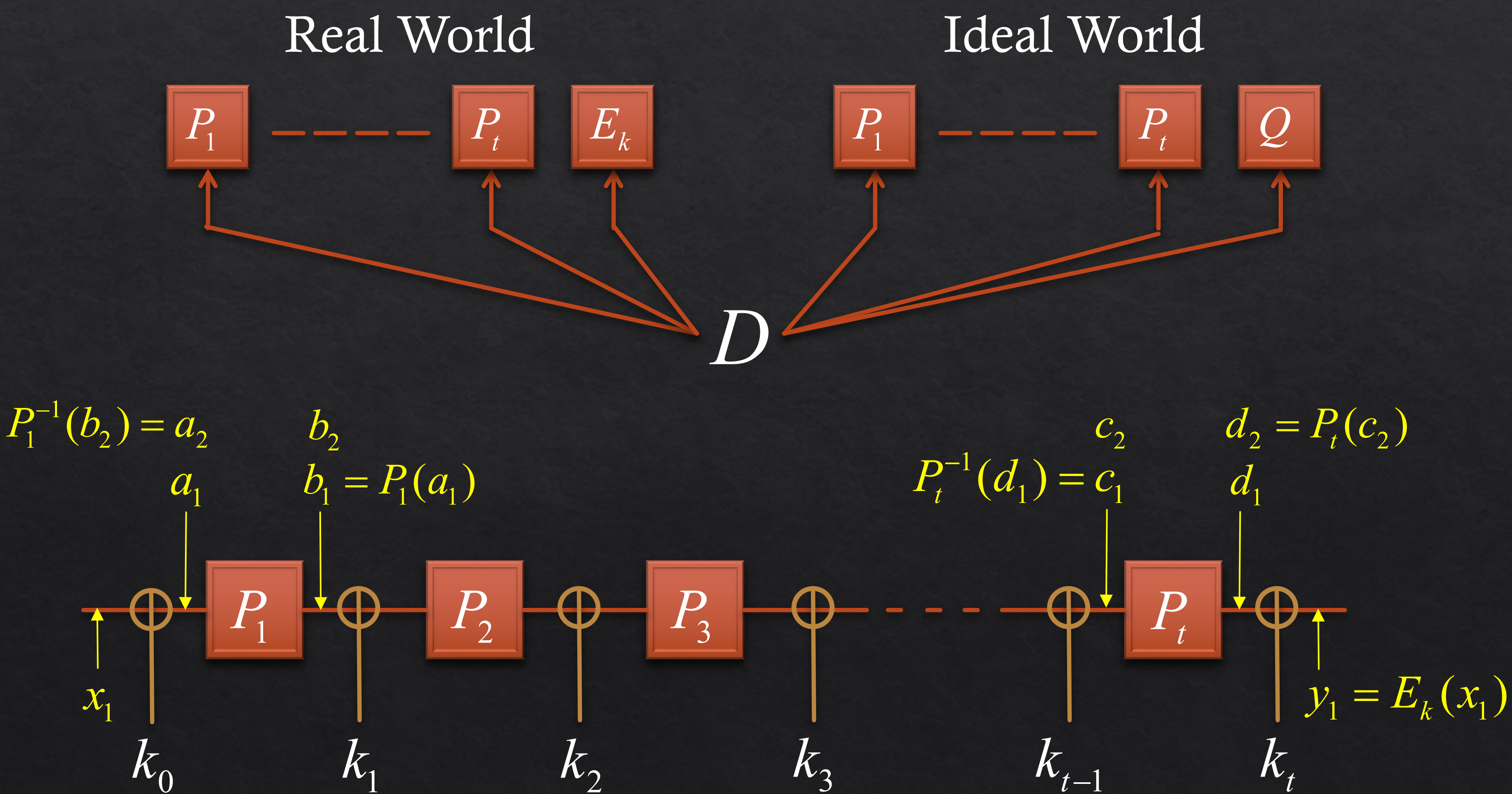
Key-Alternating Ciphers
(Ideal Permutation Model)



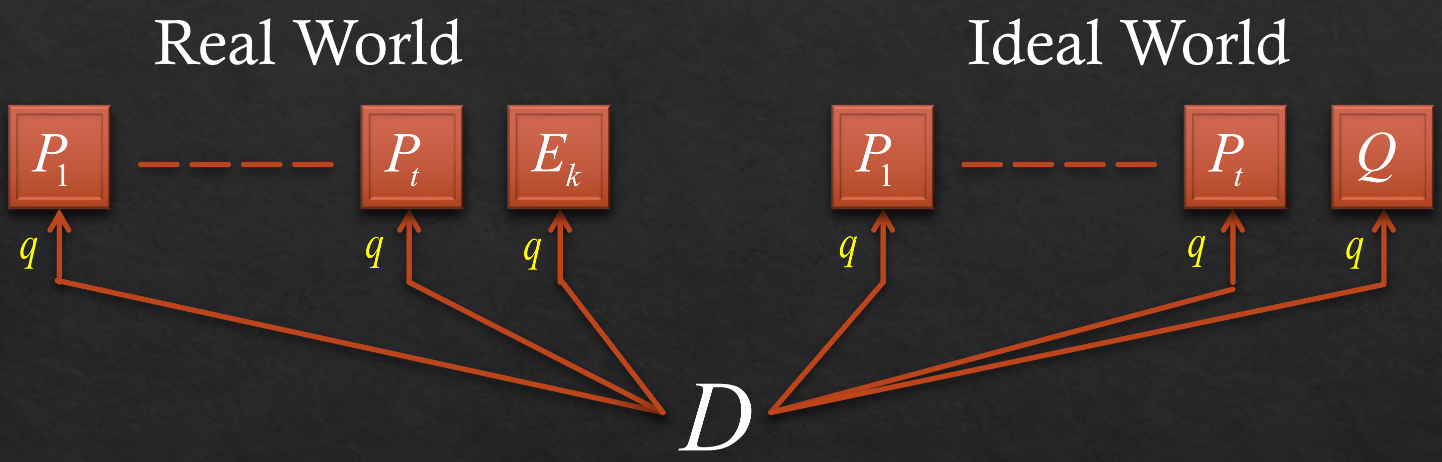
Key-Alternating Ciphers



Indistinguishability Experiment



Indistinguishability Security



$$\mathrm{Adv}(D) := \left|\Pr[D^{P_1,\cdots,P_t,E_k} = 1] - \Pr[D^{P_1,\cdots,P_t,Q} = 1]\right|$$

Previous Work

- Security: $N = 2^n$
  - $t = 1, \Omega(N^{1/2})$ [EM97]
  - $t \geq 2, \Omega(N^{2/3})$ [BKLSST12]
  - $t \geq 3, \Omega(N^{3/4})$ [S12]
  - $\forall t = 2k, \Omega(N^{t/(t+2)})$ [LPS12]
  - $\forall t, \Omega(N^{t/(t+1)})$ [CS14]

D has to make at least $N^{1/2}$ queries to distinguish the real world from the ideal world with advantage > 0.5

$$\frac{t}{t+2} = \frac{t/2}{t/2+1}$$

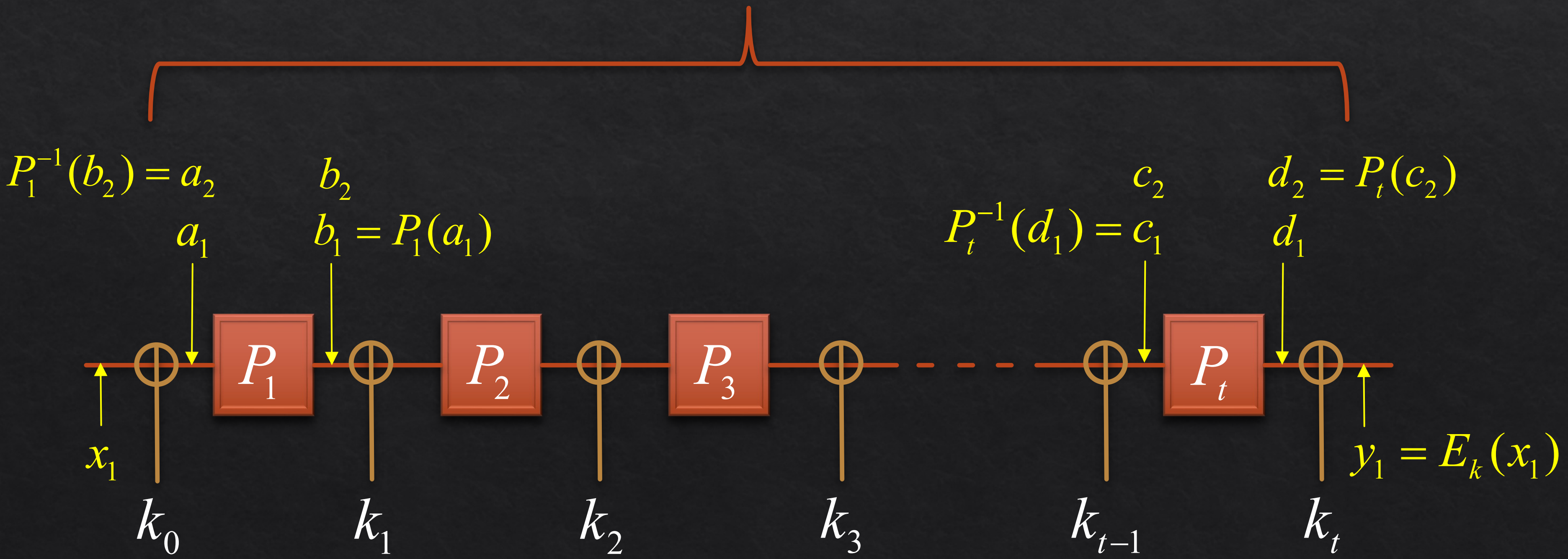
- Attack:
  - $\forall t, O(N^{t/(t+1)})$ [BKLSST12]

$N^{t/(t+1)}$ queries are sufficient to distinguish the real world from the ideal world with advantage > 0.5

Transcripts

Transcript:

$$\tau = \{(a_1, b_1), (a_2, b_2), (c_1, d_1), (c_2, d_2), (x_1, y_1)\}$$



Information-Theoretic Setting

Transcript:

$$\tau = \{(a_1, b_1), (a_2, b_2), (c_1, d_1), (c_2, d_2), (x_1, y_1)\}$$

1. No query direction   2. No query order

We can assume w.l.o.g. that D is deterministic.

$$P_2(a_2) \to b_2 \quad P_1^{-1}(d_1) \to c_1 \quad E_k(x_1) \to y_1 \ \cdots$$

Statistical Distance of Transcripts

$$\mathrm{Adv}(D) := \left|\Pr[D^{P_1,\cdots,P_t,E_k} = 1] - \Pr[D^{P_1,\cdots,P_t,Q} = 1]\right|$$

$$S = \{\tau \in \mathrm{T} : D(\tau) = 1\}$$

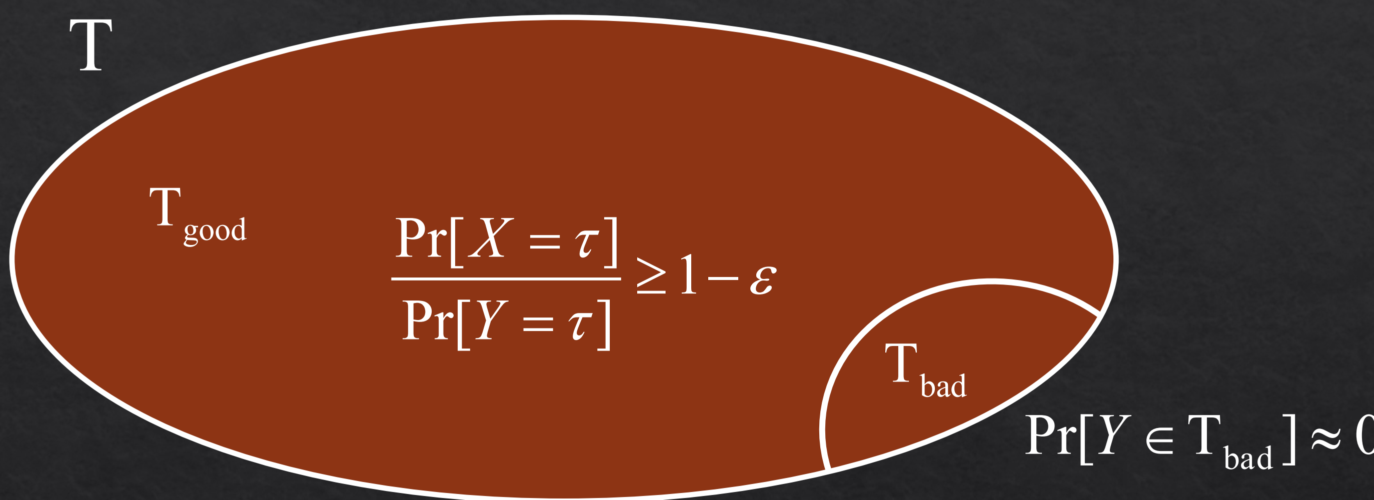
$$= \left|\Pr[X \in S] - \Pr[Y \in S]\right|$$

$$\leq \max_{S \subseteq \mathrm{T}} \left|\Pr[X \in S] - \Pr[Y \in S]\right|$$

$$= \Delta(X, Y)$$

$$\mathrm{Adv}(D) \leq \Delta(X, Y)$$

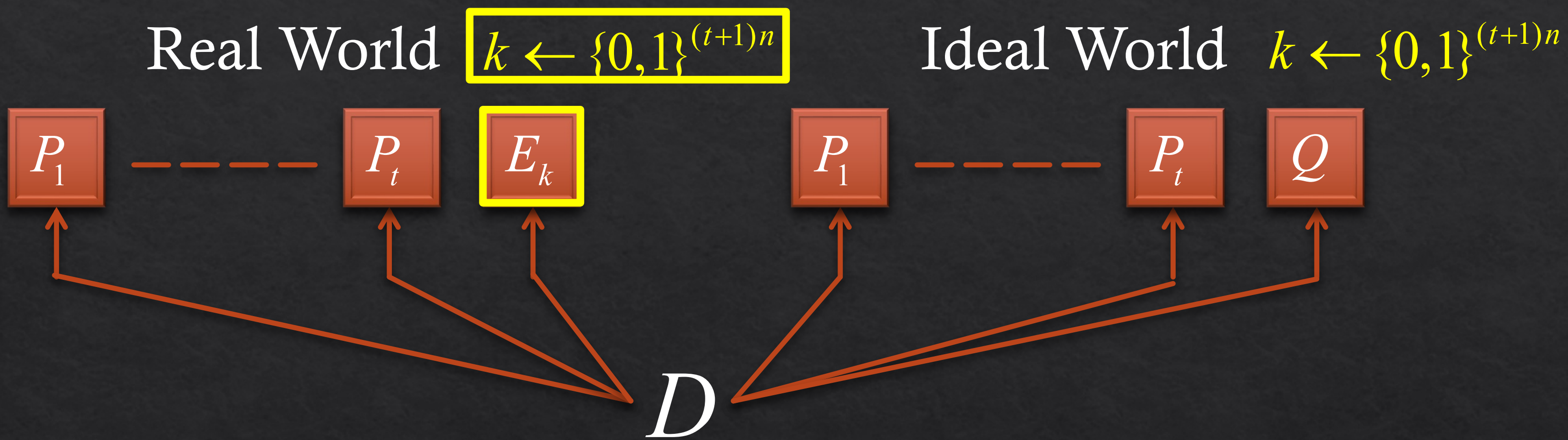
Patarin's H-coefficient Technique [P09]



$$\Delta(X,Y) \leq \varepsilon + \Pr[Y \in T_{bad}]$$

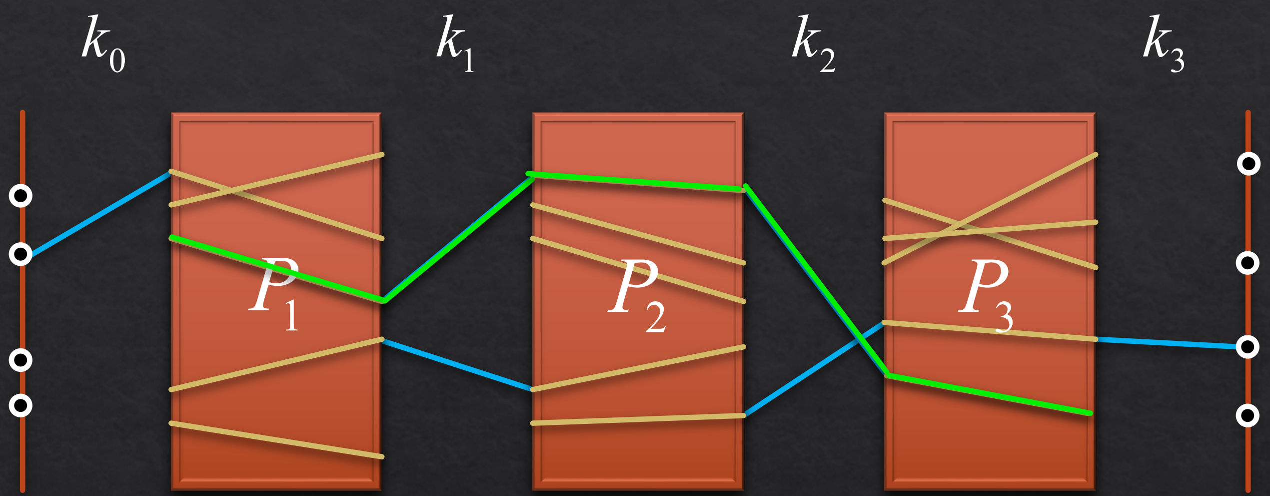
$$\Delta(X,Y) = 1 - \underset{\tau \sim Y}{E}\left[\min\left(1, \frac{\Pr[X=\tau]}{\Pr[Y=\tau]}\right)\right]$$

Reveal the Key



D is given the key for free AFTER making all of its queries

Definition of Bad Transcripts



$$\tau \in \mathrm{T}_{\text{bad}} \Leftrightarrow \exists l, \#(p_l)_\tau > C \cdot \mathop{E}_{\tau \sim Y}[\#(p_l)]$$

Example: $\mathop{E}_{\tau \sim Y}[\#(p_3)] = \frac{q^3}{N^2}$ $\quad \#(p_3)_\tau > C\frac{q^3}{N^2}$

Markov Inequality $\Rightarrow \Pr[Y \in \mathrm{T}_{\text{bad}}] = O(t^2)\frac{1}{C} \approx 0$

Lower Bounding the Probability Ratio for Good Transcripts (Major Challenge)

$$\frac{\Pr[X = \tau]}{\Pr[Y = \tau]} \geq 1 - \varepsilon$$

Lower Bounding the Probability Ratio for Good Transcripts (Major Challenge)

$$\tau = \left\{ \begin{array}{ccccc} \tau_1 & \tau_2 & & \tau_t & \tau_0 \\ (u_1^1, v_1^1) & (u_1^2, v_1^2) & \cdots & (u_1^t, v_1^t) & (x_1, y_1) \\ (u_2^1, v_2^1) & (u_2^2, v_2^2) & \cdots & (u_2^t, v_2^t) & (x_2, y_2) \\ \vdots & \vdots & \cdots & \vdots & \vdots \\ (u_q^1, v_q^1) & (u_q^2, v_q^2) & \cdots & (u_q^t, v_q^t) & (x_q, y_q) \\ P_1 & P_2 & & P_t & E_k / Q \end{array} \right\} \cup \{k^*\}$$

$$\frac{\Pr[X = \tau]}{\Pr[Y = \tau]} = \frac{\Pr[E_k \triangleright \tau_0, P_1 \triangleright \tau_1, \cdots, P_t \triangleright \tau_t, k = k^*]}{\Pr[Q \triangleright \tau_0, P_1 \triangleright \tau_1, \cdots, P_t \triangleright \tau_t, k = k^*]}$$

$$= \frac{\Pr[E_k \triangleright \tau_0 \mid P_1 \triangleright \tau_1, \cdots, P_t \triangleright \tau_t, k = k^*]}{\Pr[Q \triangleright \tau_0 \mid P_1 \triangleright \tau_1, \cdots, P_t \triangleright \tau_t, k = k^*]} = \frac{\Pr[E_k \triangleright \tau_0 \mid G]}{\Pr[Q \triangleright \tau_0 \mid G]}$$

Lower Bounding the Probability Ratio for Good Transcripts (Major Challenge)

$$\frac{\Pr[X=\tau]}{\Pr[Y=\tau]} = \frac{\Pr[E_k \triangleright \tau_0 \mid G]}{\Pr[Q \triangleright \tau_0 \mid G]} \geq 1-\varepsilon \qquad G \Leftrightarrow P_1 \triangleright \tau_1, \cdots, P_t \triangleright \tau_t, k = k^*$$

$$\tau_0 = \{(x_1, y_1), (x_2, y_2), \cdots, (x_q, y_q)\}$$

Ideal World

$$\Pr[Q \triangleright \tau_0 \mid G] = \Pr[Q \triangleright \tau_0] = \Pr[x_1 \to y_1, x_2 \to y_2, \cdots, x_q \to y_q]$$

$$= \frac{1}{N} \cdot \frac{1}{N-1} \cdots \frac{1}{N-q+1}$$

Lower Bounding the Probability Ratio for Good Transcripts (Major Challenge)

$$\frac{\Pr[X=\tau]}{\Pr[Y=\tau]}=\frac{\Pr[E_k \triangleright \tau_0 \mid G]}{\Pr[Q \triangleright \tau_0 \mid G]} \geq 1-\varepsilon \qquad G \Leftrightarrow P_1 \triangleright \tau_1, \cdots, P_t \triangleright \tau_t, k=k^*$$

$$\tau_0=\{(x_1,y_1),(x_2,y_2),\cdots,(x_q,y_q)\}$$

Ideal World

$$\Pr[Q \triangleright \tau_0 \mid G]=\Pr[Q \triangleright \tau_0]=\Pr[x_1 \to y_1, x_2 \to y_2, \cdots, x_q \to y_q]$$

$$= \Pr[x_1 \to y_1] \qquad =1/N$$

$$\times \Pr[x_2 \to y_2 \mid x_1 \to y_1] \qquad =1/(N-1)$$

$$\vdots$$

$$\times \Pr[x_q \to y_q \mid x_i \to y_i, i<q] \qquad =1/(N-q+1)$$

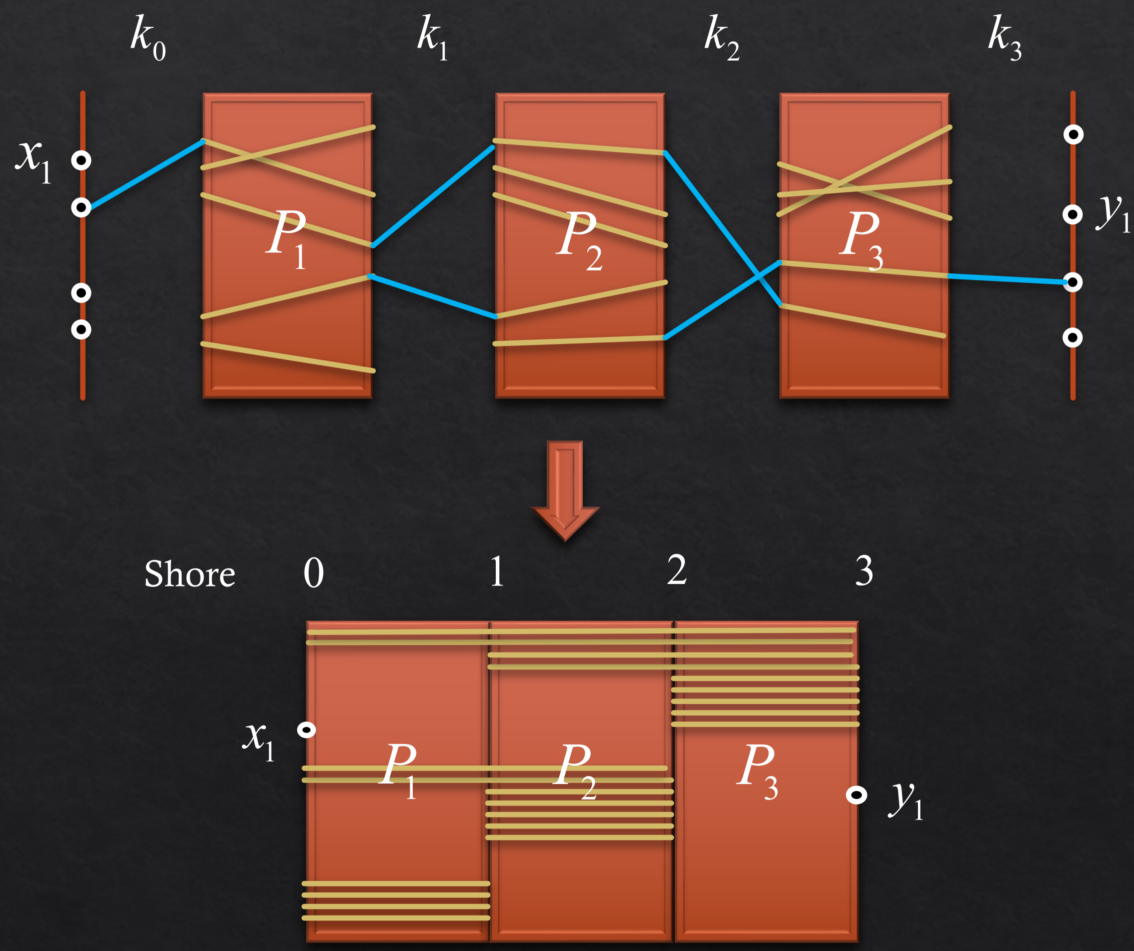
Lower Bounding the Probability Ratio for Good Transcripts (Major Challenge)

$$\frac{\Pr[X=\tau]}{\Pr[Y=\tau]}=\frac{\Pr[E_k \rhd \tau_0 \mid G]}{\Pr[Q \rhd \tau_0 \mid G]}\geq 1-\varepsilon \qquad G \Leftrightarrow P_1 \rhd \tau_1,\cdots,P_t \rhd \tau_t, k=k^*$$

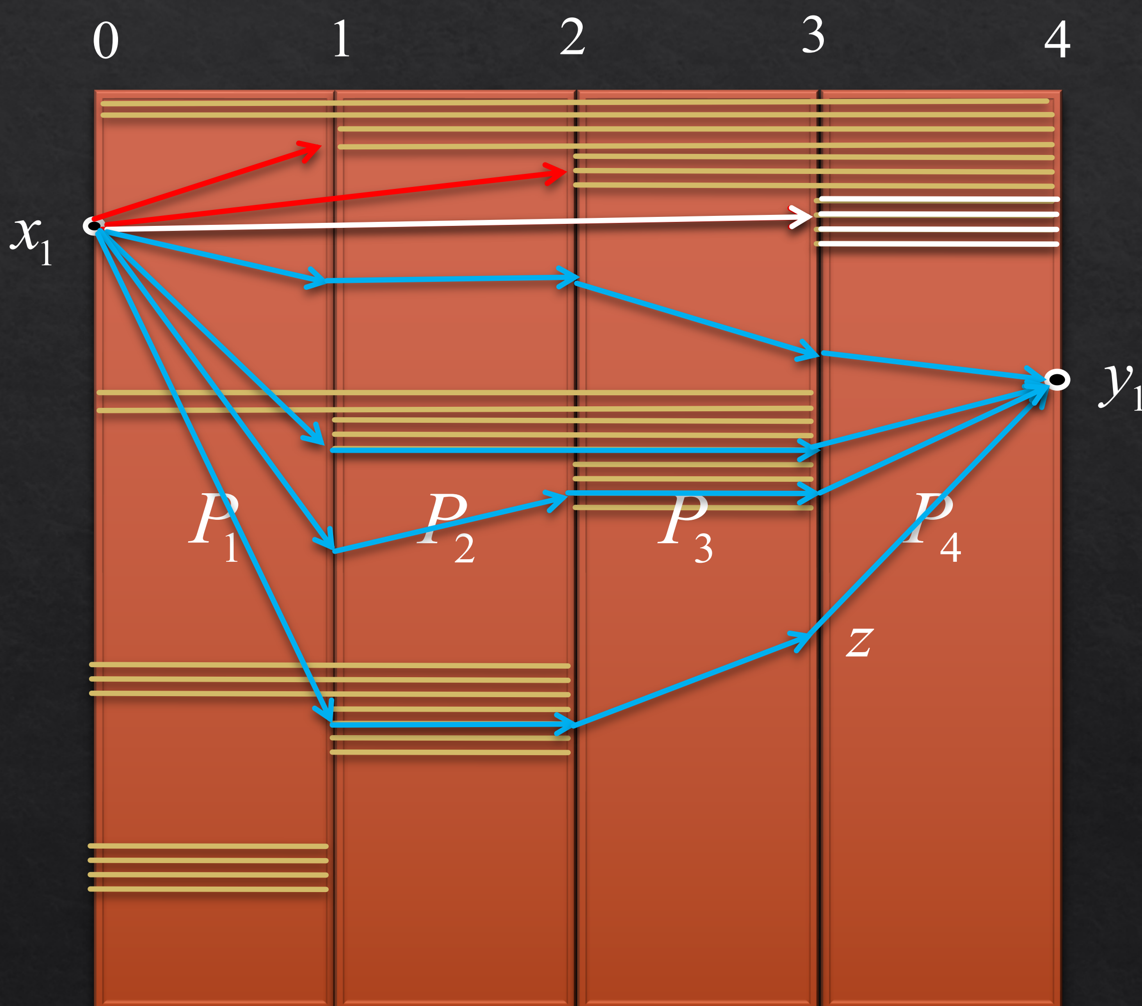
$$\tau_0=\{(x_1,y_1),(x_2,y_2),\cdots,(x_q,y_q)\}$$

Ideal World		Real World
$\Pr[Q \rhd \tau_0 \mid G]$		$\Pr[E_k \rhd \tau_0 \mid G]$
$=\Pr[x_1 \to y_1]$	$=1/N$	$=\boxed{\Pr[x_1 \to y_1 \mid G]}$
$\times \Pr[x_2 \to y_2 \mid x_1 \to y_1]$	$=1/(N-1)$	$\times \Pr[x_2 \to y_2 \mid x_1 \to y_1, G]$
$\vdots$		$\vdots$
$\times \Pr[x_q \to y_q \mid x_i \to y_i, i<q]$	$=1/(N-q+1)$	$\times \Pr[x_q \to y_q \mid x_i \to y_i, i<q, G]$

Lower Bounding the Probability Ratio for Good Transcripts (Major Challenge)

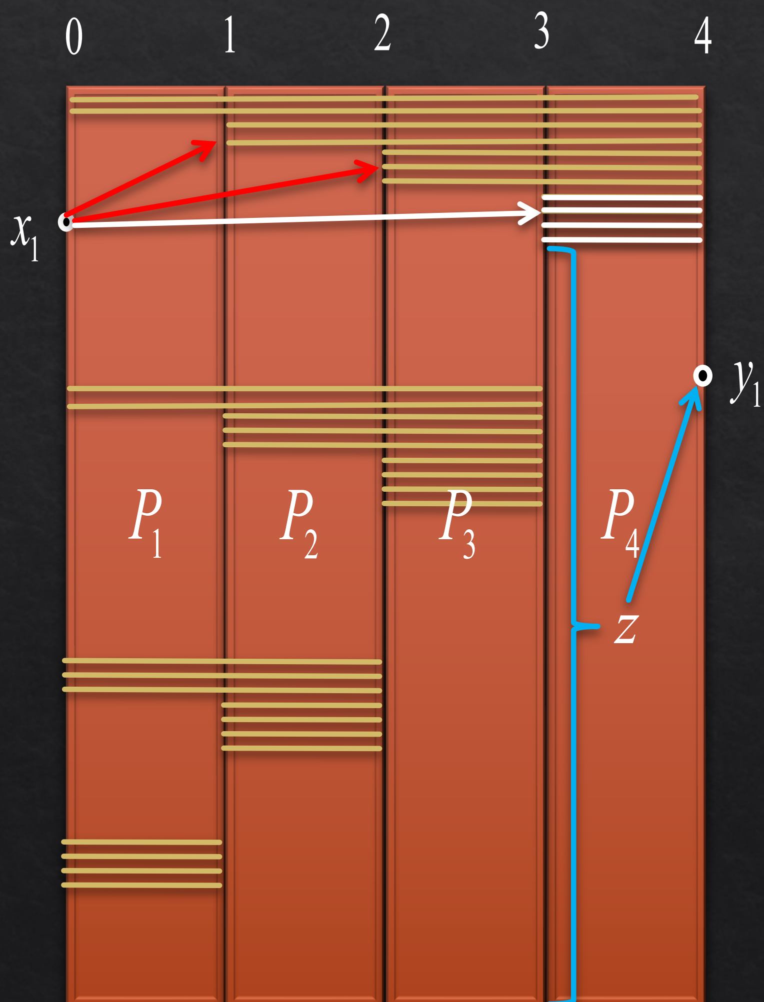


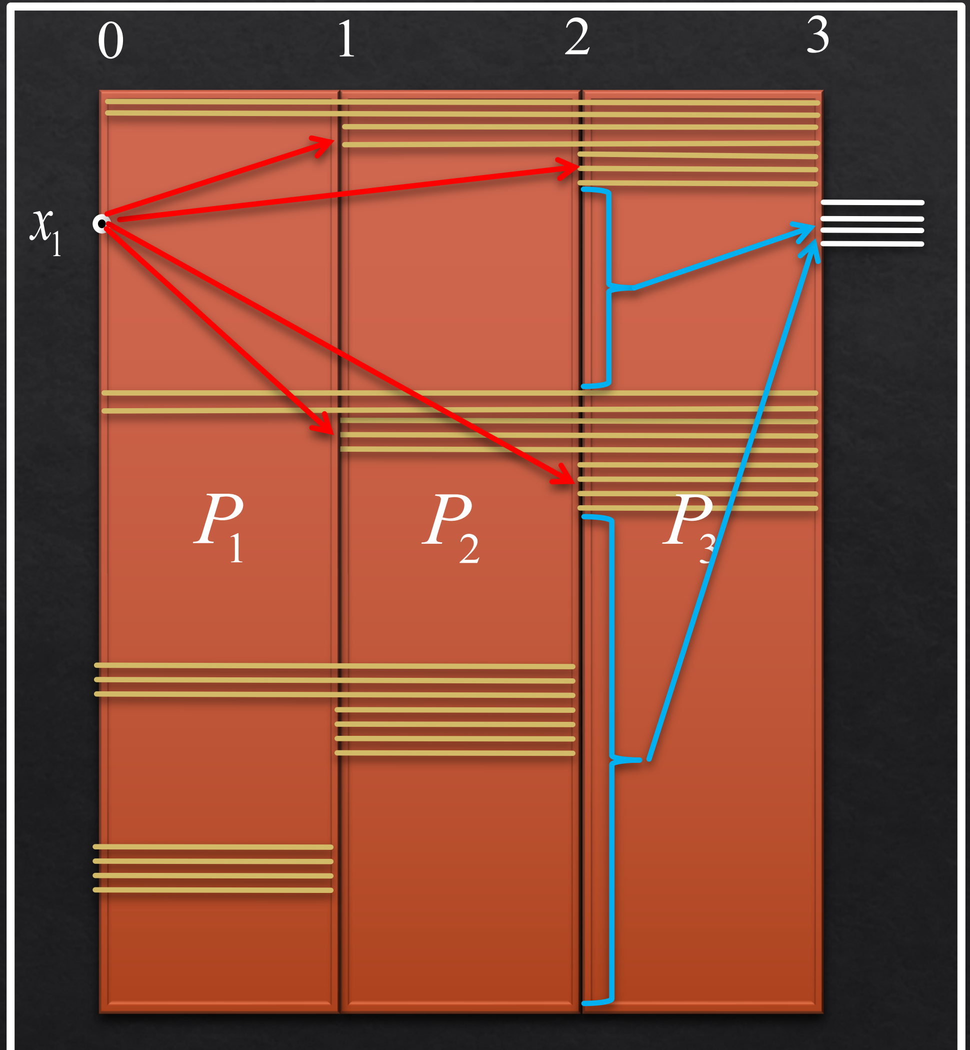
Lower Bounding the Probability Ratio for Good Transcripts (Major Challenge)



Q: What is the probability of z being free?

Lower Bounding the Probability Ratio for Good Transcripts (Major Challenge)





Summary

- Tight security bounds for key-alternating ciphers

$$\mathrm{Adv}(D) = O(1)\frac{q^{t+1}}{N^t} + O(1)$$

$$\Omega(N^{t/(t+1)})$$

- Patarin's H-coefficient Technique

The End

Thanks & Any Questions?