Reliable, Deniable, and Hidable Communication

Mayank Bakshi

The Chinese University of Hong Kong

Joint work with

Alex Sprintson

Swanand Kadhe

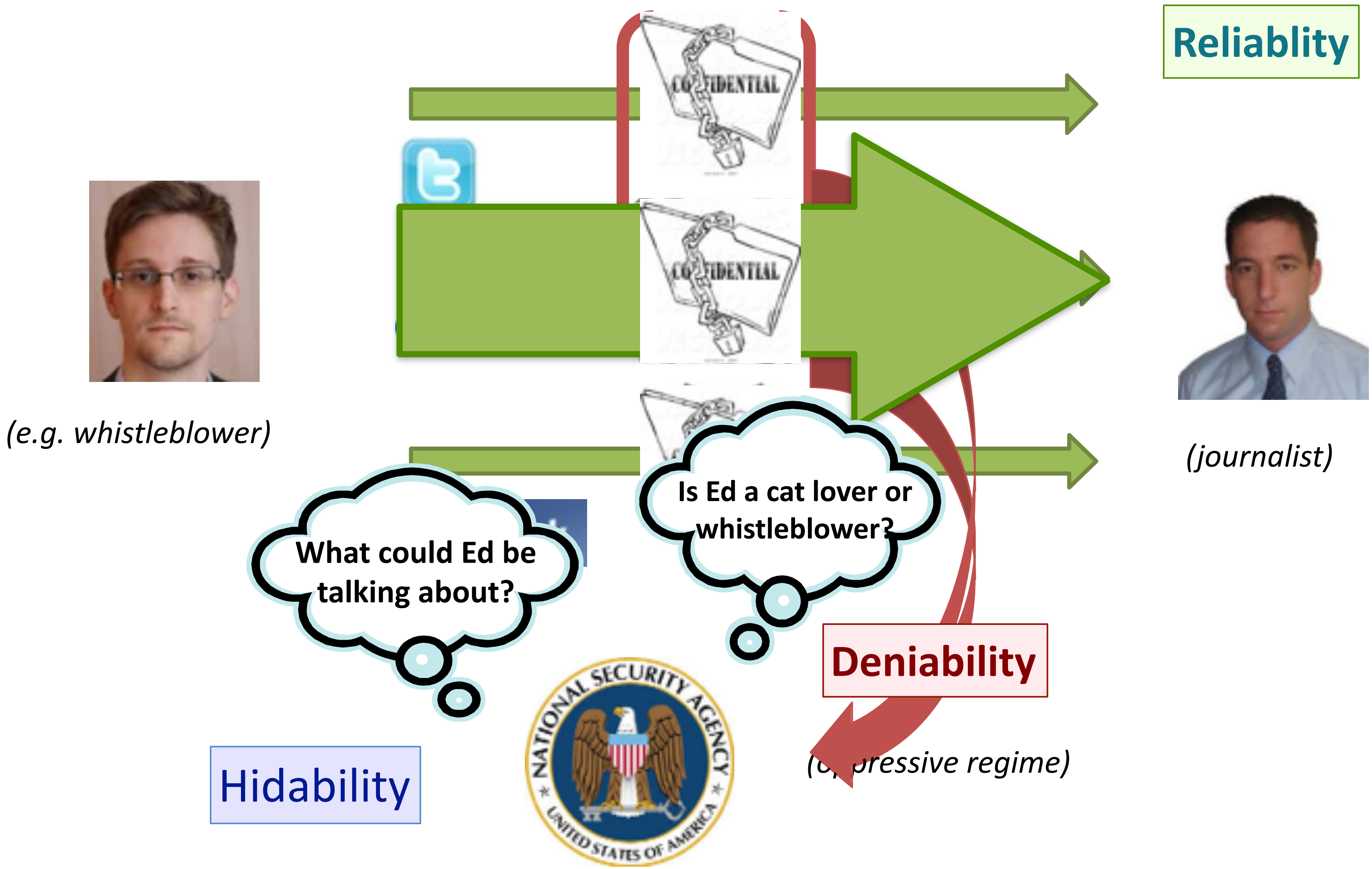
Sid Jaggi

(Howard) Pak Hou Che

Chung Chan

Tracey Ho

Motivating Scenario



Anonymity

Hide within a crowd

Privacy

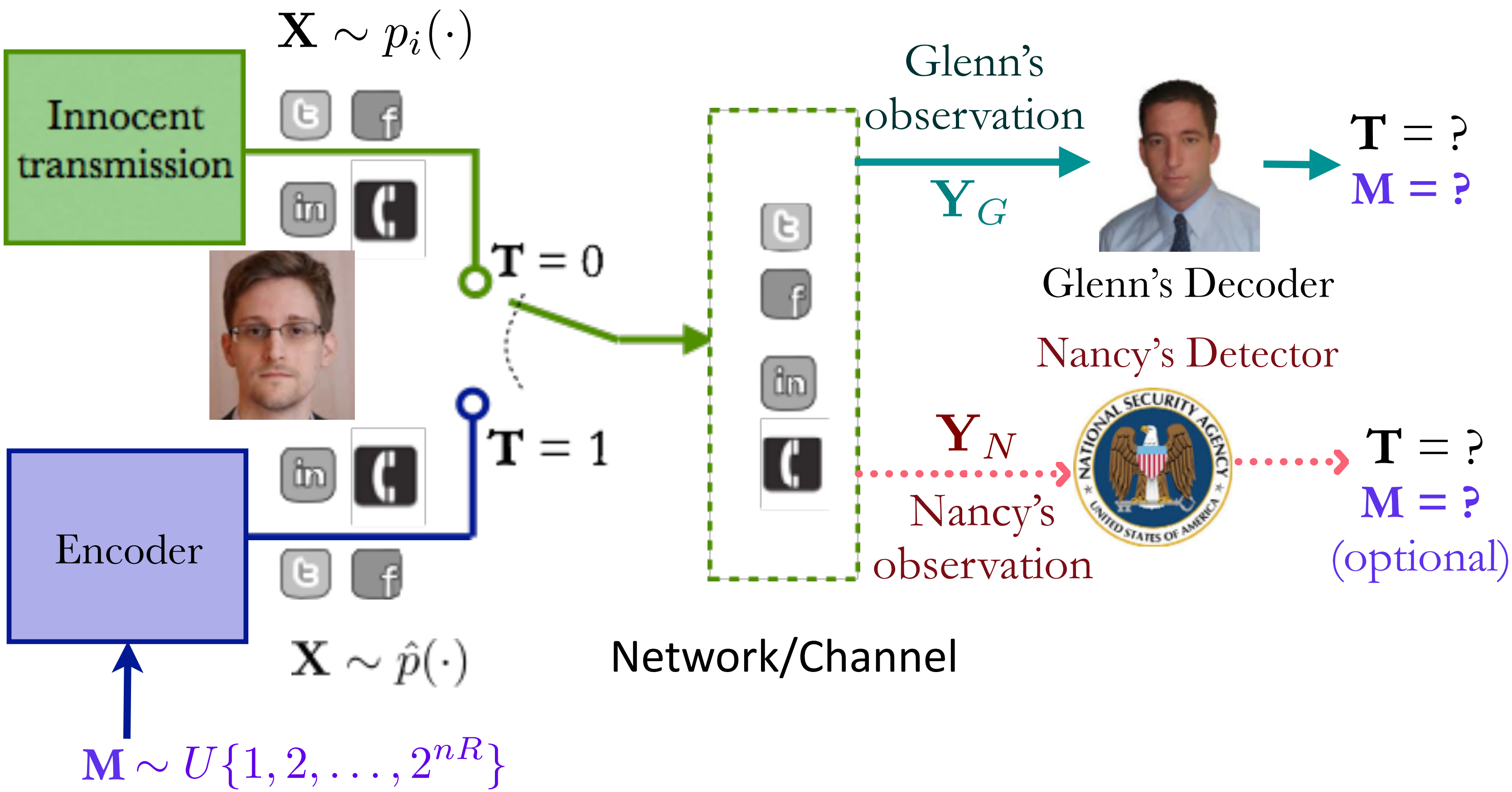
Steganography

Deniability

Hide messages in a cover text

Hidability

Problem Formulation



Goals:

1. Reliability : $\sum_{t \in \{0,1\}} \Pr(\hat{T} \neq T | T = t) + \Pr(\hat{M} \neq M | \hat{T} = 1) < \epsilon_1$

$T \in \{0, 1\}$: Ed's Transmission Status

Estimate T — Estimate M

2. Deniability : $\mathcal{V}(p_i(\mathbf{Y}_N), \hat{p}(\mathbf{Y}_N)) < \epsilon_2$

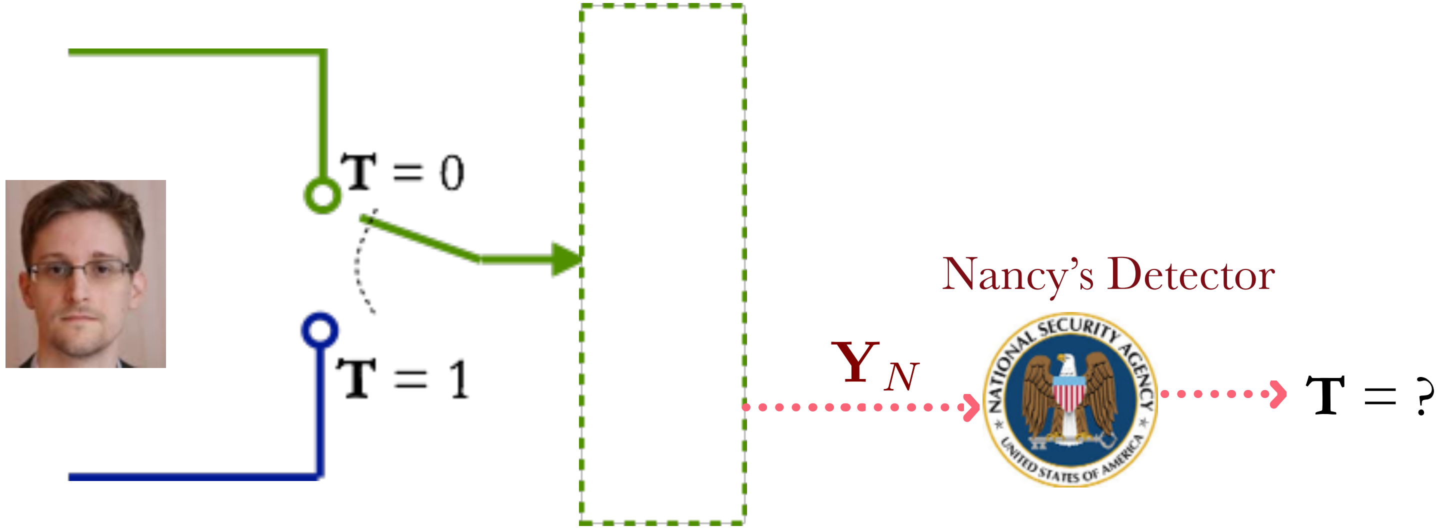
$p_i(\cdot)$: innocent distribution (i.i.d)

$\hat{p}(\cdot)$: active distribution (n-letter)

3. Hidability : $\frac{(1 - \epsilon_3)}{2^{nR}} < \Pr(M = m | \mathbf{Y}_w = \mathbf{y}, T = 1) < \frac{(1 + \epsilon_3)}{2^{nR}} \quad \forall m \in \{0, 1\}^{nR}$

Variational distance: $\frac{1}{2} ||p_i(\mathbf{Y}_w) - \hat{p}(\mathbf{Y}_w)||_1$

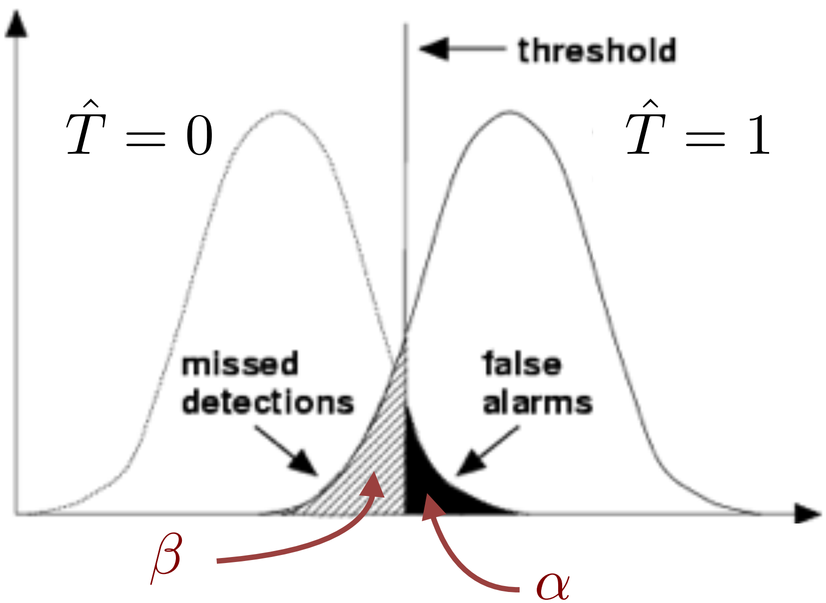
Deniability



Want:

- Nancy's best $\hat{T}$ no better than "*random*"
- Nancy performs Hypothesis Testing
- Trivially, $\alpha + \beta \leq 1$

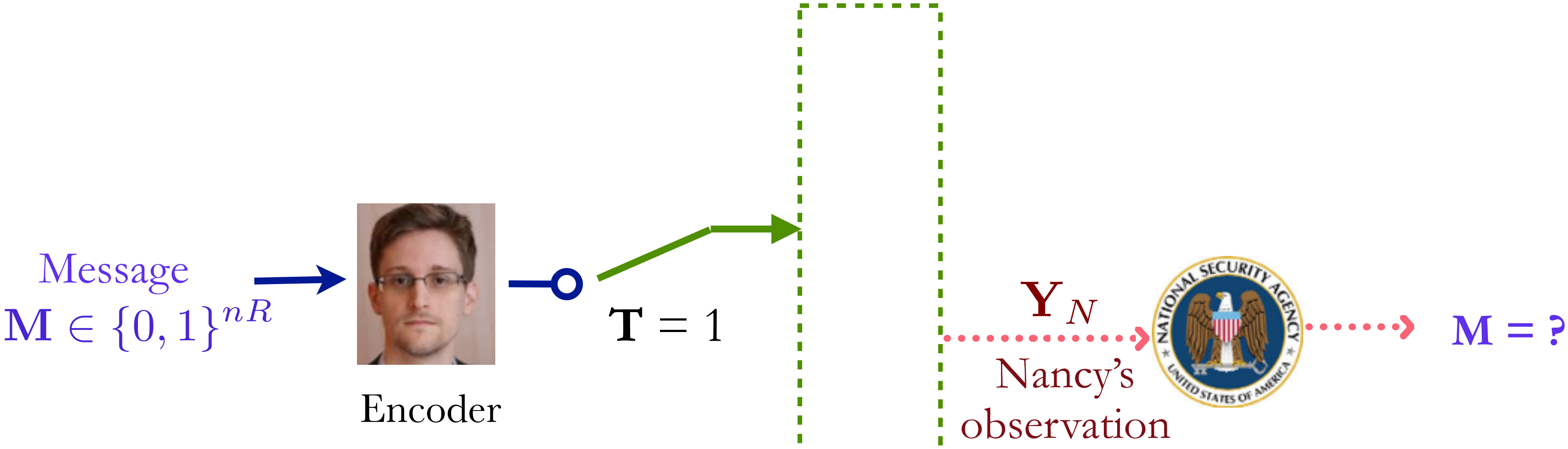
Ensure: $\mathbb{V}\left(p_i(\mathbf{Y}_N), \hat{p}(\mathbf{Y}_N)\right) < \epsilon$ / $(\alpha + \beta) > 1 - \epsilon$ for best $\hat{T}$



Hypothesis Testing:

$$(\alpha + \beta) = 1 - \mathbb{V}\left(p_i(\mathbf{Y}_N), \hat{p}(\mathbf{Y}_N)\right)$$

Hidability



Strong secrecy: $I(\mathbf{M}; \mathbf{Y}_N) < \epsilon$

New secrecy metric: "Super-strong secrecy"

$$\frac{1-\epsilon}{2^{nR}} < \frac{\Pr(\mathrm{M} = m | \mathbf{Y}_N = \mathbf{y}, T = 1)}{\Pr(\mathrm{M} = m | T = 1)} < \frac{1+\epsilon}{2^{nR}} \qquad \forall\, m$$

Nancy cannot test if m is the message

Hidability

Super-strong secrecy

$$\frac{1-\epsilon}{2^{nR}} < \Pr(\mathrm{M} = m | \mathbf{Y}_N = \mathbf{y}, T = 1) < \frac{1+\epsilon}{2^{nR}}$$

Strong secrecy

$$I(\mathbf{M}; \mathbf{Y}_N) < \epsilon$$

Super strong secrecy ⇒ Strong secrecy

Super strong secrecy ⇍ Strong secrecy

- e.g. Encode every message except one

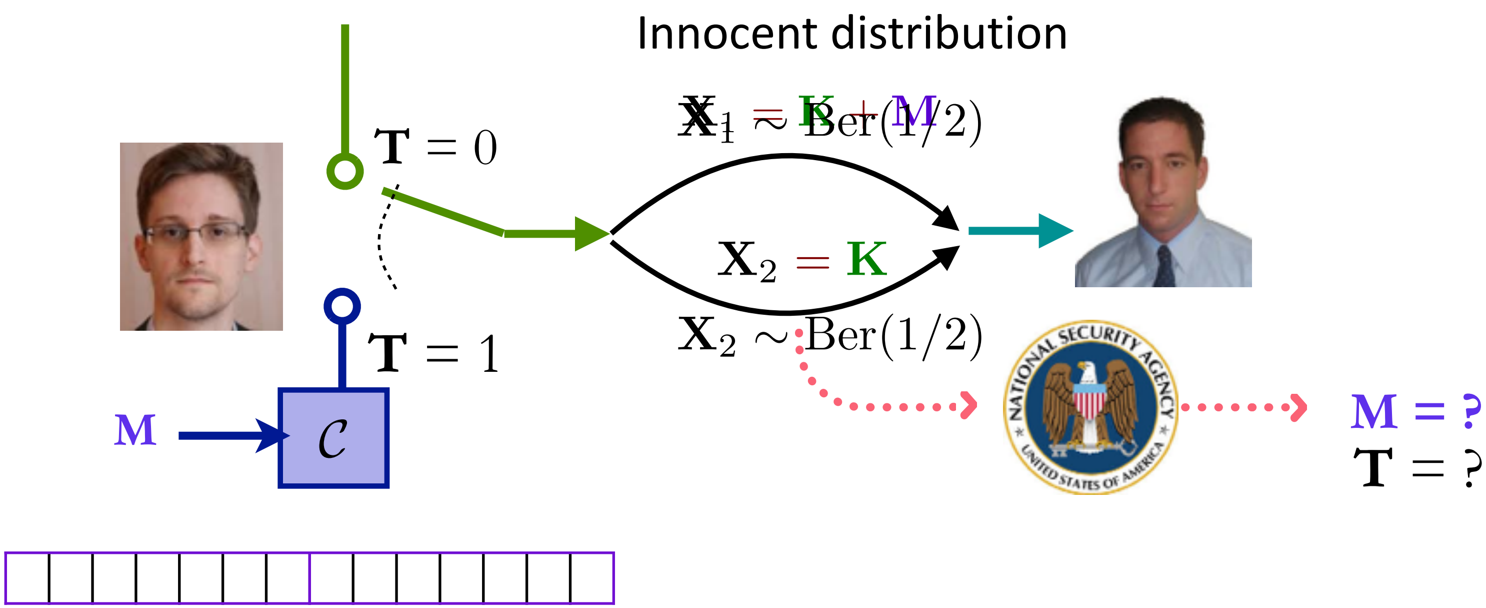
$$\begin{aligned} 1 &\longrightarrow \mathbf{X}(1) \\ 2 &\longrightarrow \mathbf{X}(2) \\ &\vdots \\ (2^{nR}-1) &\longrightarrow \mathbf{X}(2^{nR}-1) \\ 2^{nR} &\longrightarrow 2^{nR} \end{aligned}$$

$$\begin{aligned} I(M; \mathbf{Y}_N) &= \sum_{m,y} p(m,y) \log \frac{p(m|y)}{p(m)} \\ &= \sum_{m,y} p(m)p(y)(1 \pm \epsilon) \log(1 \pm \epsilon) \\ &= (1 \pm \epsilon) \log(1 \pm \epsilon) \end{aligned}$$

Strong secrecy ✓

Super-strong secrecy ✗

Hidability vs Deniability



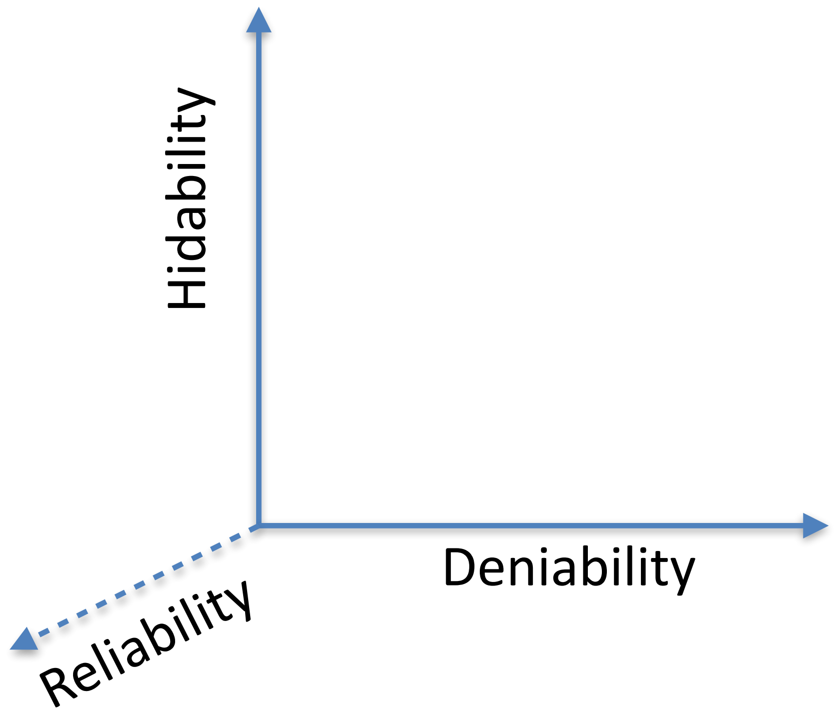
$2n$ bits

Hidability ⇏ Deniability

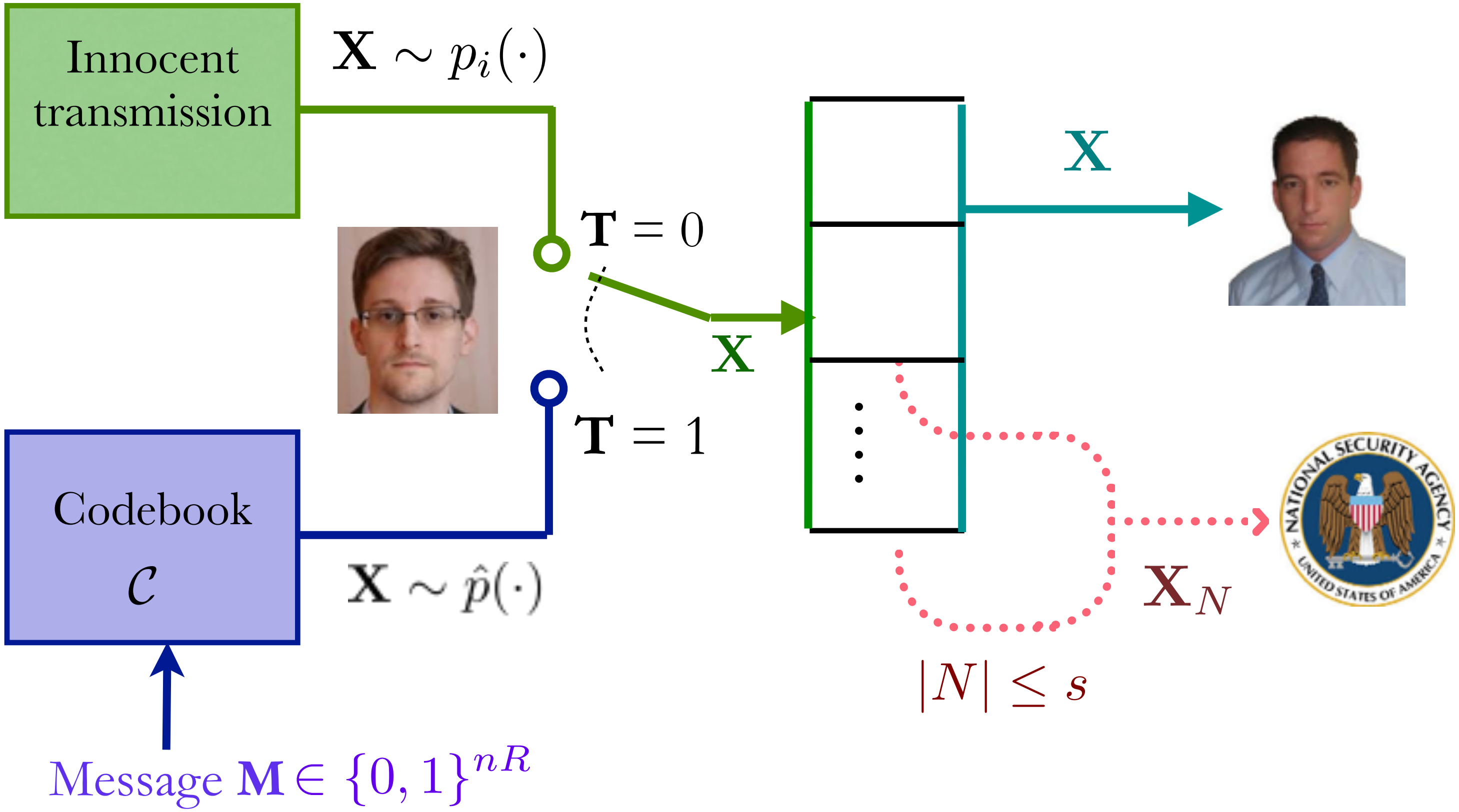
Codes for Hidability don't look innocent

Innocent distribution = Codeword distribution

Hidability vs Deniability



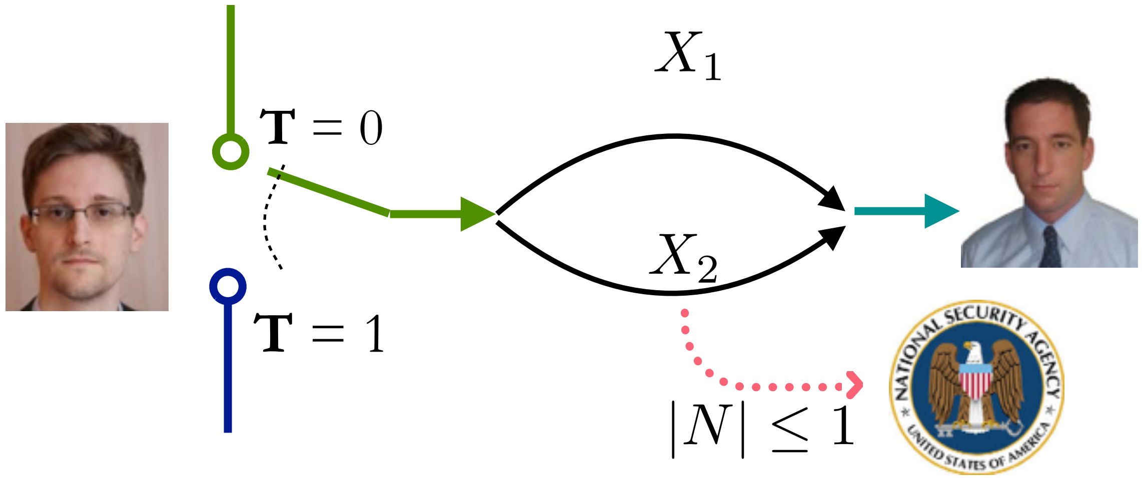
Network of parallel links



Deniability $\Leftrightarrow$ $\mathbb{V}\left(p_i(\mathbf{Y}_N), \hat{p}(\mathbf{Y}_N)\right) < \epsilon$ $\Leftrightarrow$ $\mathbb{V}\left(p_i(\mathbf{X}_N), \hat{p}(\mathbf{X}_N)\right) < \epsilon_2 \ \forall \ |N| \leq s$

$\Rightarrow$ Ed's strategy: Pretend innocence, i.e. set $p_i(X_N) \approx \hat{p}(X_N)$

Example: Two links



Given:

$$p_i(x_1, x_2)$$

x_2 \ x_1	0	1	
0	*1/12*	*1/4*	
1	*1/4*	*5/12*	

Design:

$$\hat{p}(x_1, x_2)$$

x_2 \ x_1	0	1	
0	*1/9*	*2/9*	
1	*2/9*	*4/9*	

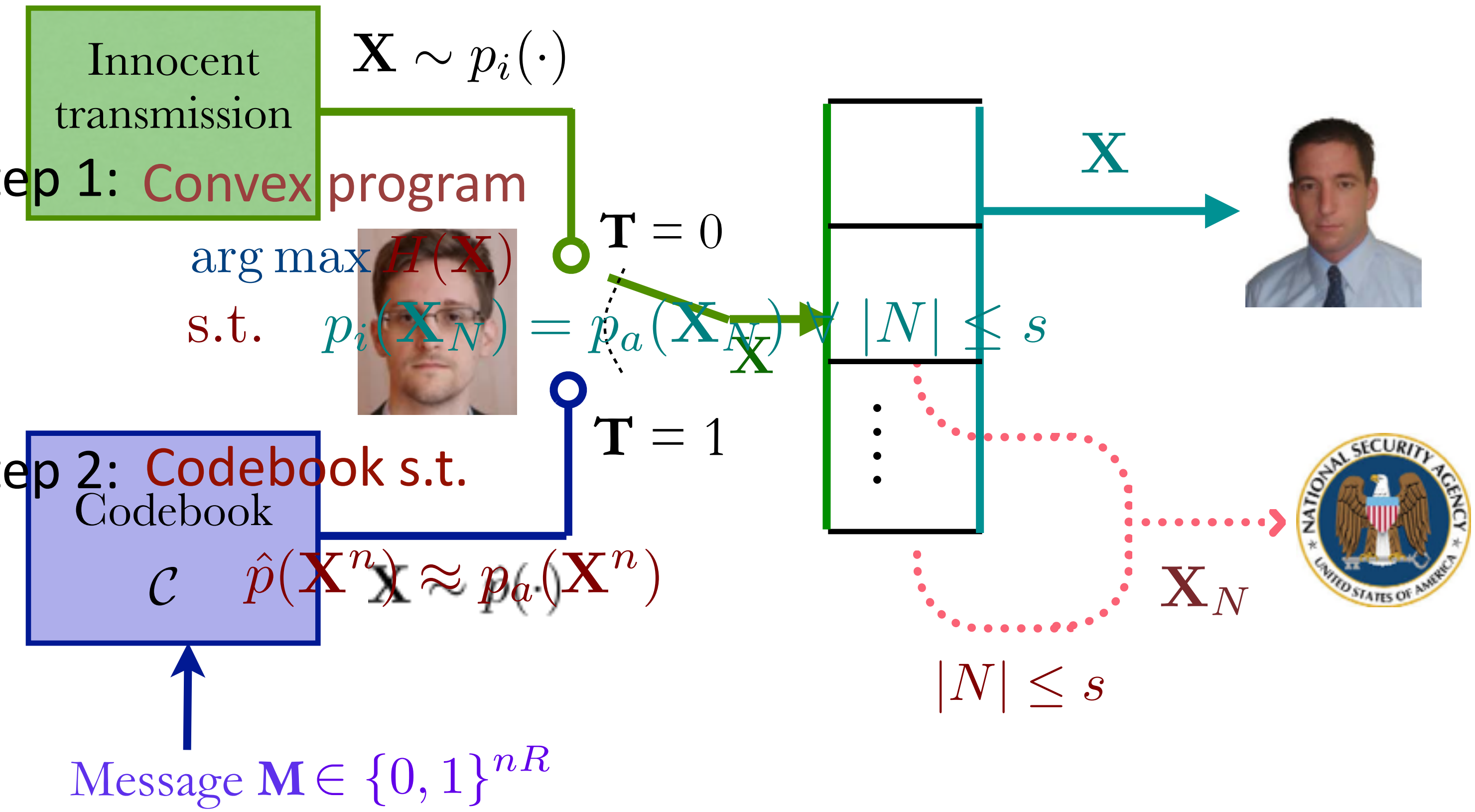
Network of parallel links

Step 1: Convex program

$\arg\max H(\mathbf{X})$

s.t. $p_i(\mathbf{X}_N) = p_a(\mathbf{X}_N) \ \forall \ |N| \leq s$

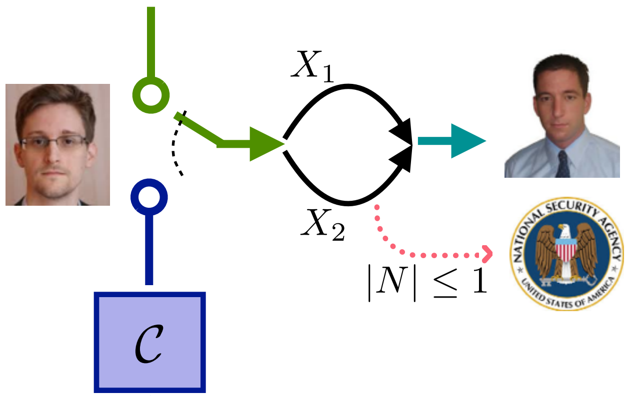
Step 2: Codebook s.t. $\hat{p}(\mathbf{X}^n) \approx p_a(\mathbf{X}^n)$



Deniability $\Leftrightarrow$ $\mathbb{V}\left(p_i(\mathbf{Y}_N), \hat{p}(\mathbf{Y}_N)\right) < \epsilon$ $\Leftrightarrow$ $\mathbb{V}\left(p_i(\mathbf{X}_N), \hat{p}(\mathbf{X}_N)\right) < \epsilon_2 \ \forall \ |N| \leq s$

$\Rightarrow$ Ed's strategy: Pretend innocence, i.e. set $p_i(X_N) \approx \hat{p}(X_N)$

Example: Two links



$\mathbf{M} \sim U\{1, 2, \ldots, 2^{nR}\}$

x_2 \ x_1	0	1	
0	1/12	1/4	1/3
1	1/4	5/12	2/3
	1/3	2/3	

$p_i(x_1, x_2)$

x_2		1	
0	1/3	2/9	1/3
1	2/3	4/9	2/3
	optimal $p_a(x_2)$ 1/3	2/3	

optimal $p_a(x_1, x_2)$

Want: $M \xrightarrow{\mathcal{C}} X_2$

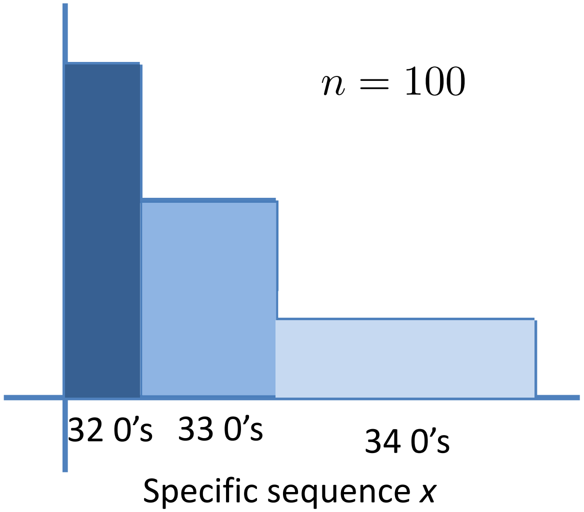
$U\{\ldots\} \rightarrow \hat{p}(\mathbf{X}_2^n)$ s.t. $\mathbb{V}\left(\hat{p}(\mathbf{X}_2^n), p_a(\mathbf{X}_2^n)\right) < \epsilon$

Example: Two links

Attempt 1: Use sequences with exactly 1/3 zeroes

x_2	
0	***1/3***
1	***2/3***

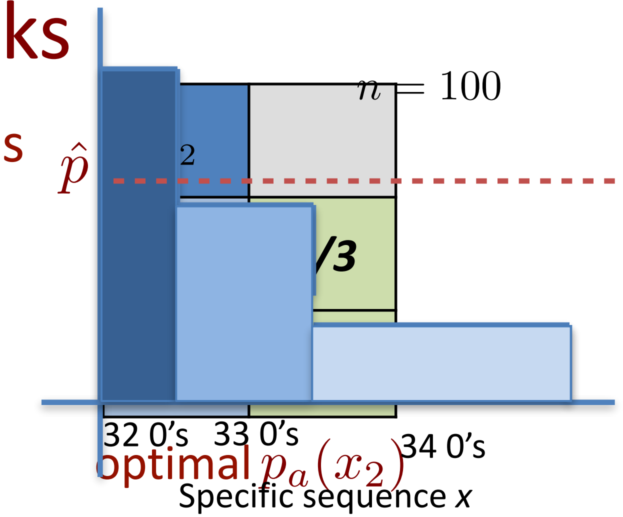
optimal $p_a(x_2)$



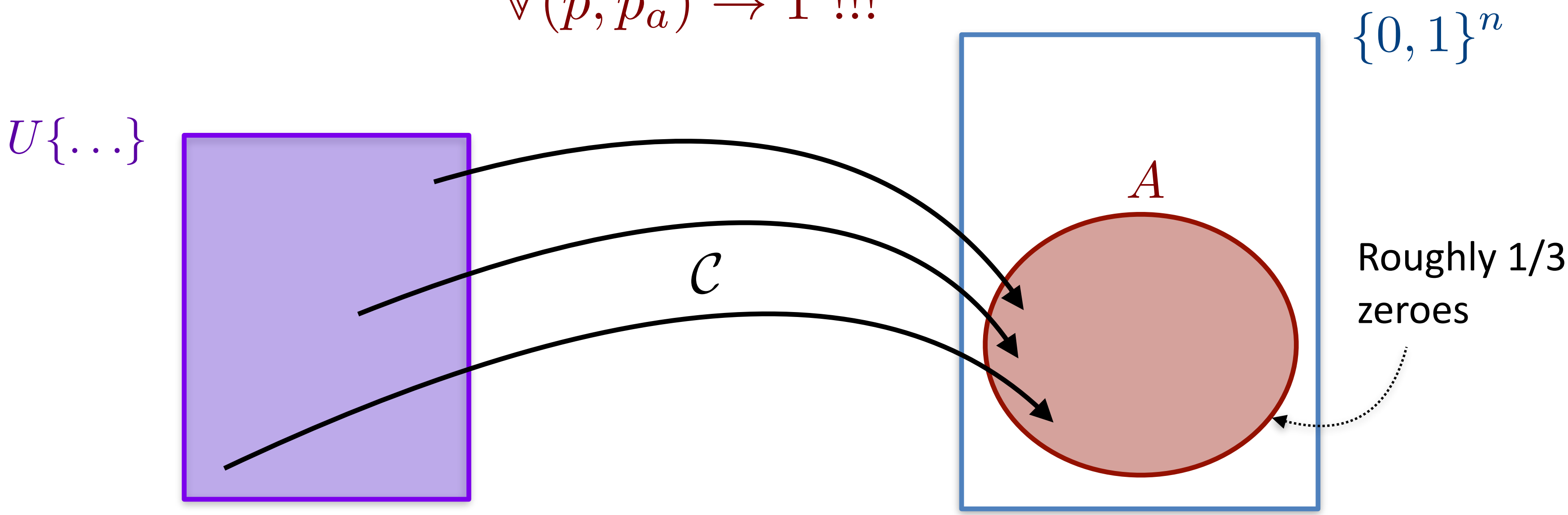
$$p_a(X_2^n \in T) = O(1/\sqrt{n}) \Longrightarrow \mathbb{V}(\hat{p}, p_a) \to 1 \text{ !!!}$$

Example: Two links

Attempt 2: Use sequences with approx 1/3 zeroes



$$\mathbb{V}(\hat{p}, p_a) \to 1 \text{ !!!}$$

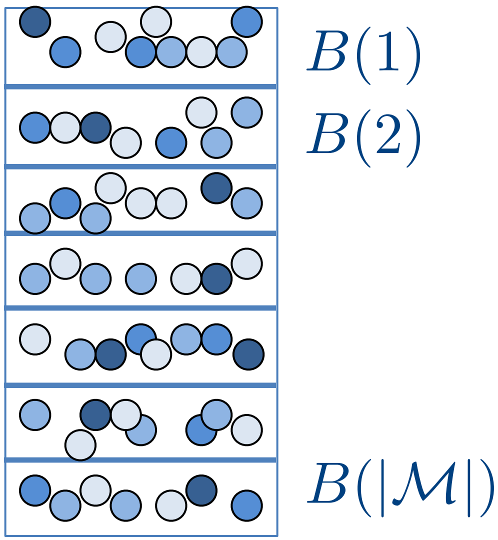


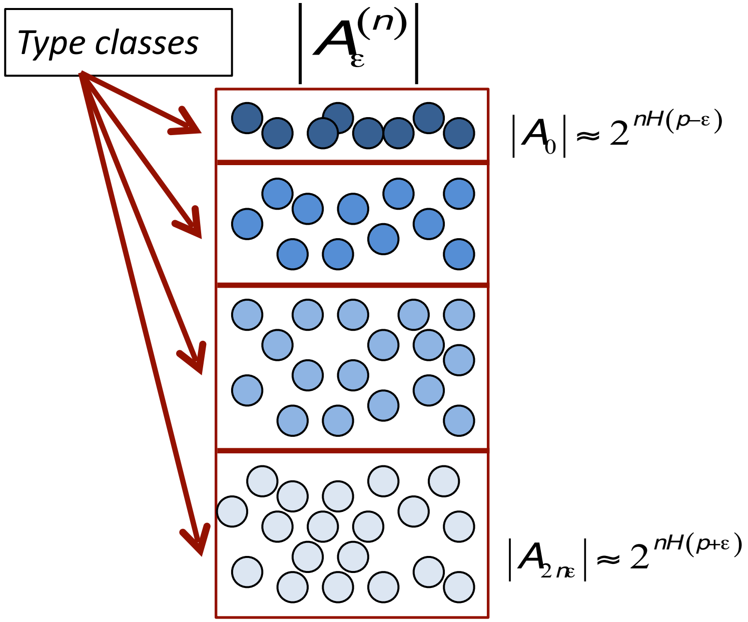
Example: Two links

Attempt 3: Stochastic Encoding

Encoder: $$p(\mathbf{x}|m) = \frac{p_a(\mathbf{x})}{p_a(B(m))} \quad \text{if } \mathbf{x} \in B(m)$$

$$|\mathcal{M}| = 2^{n(H(p_a)-\delta)}$$

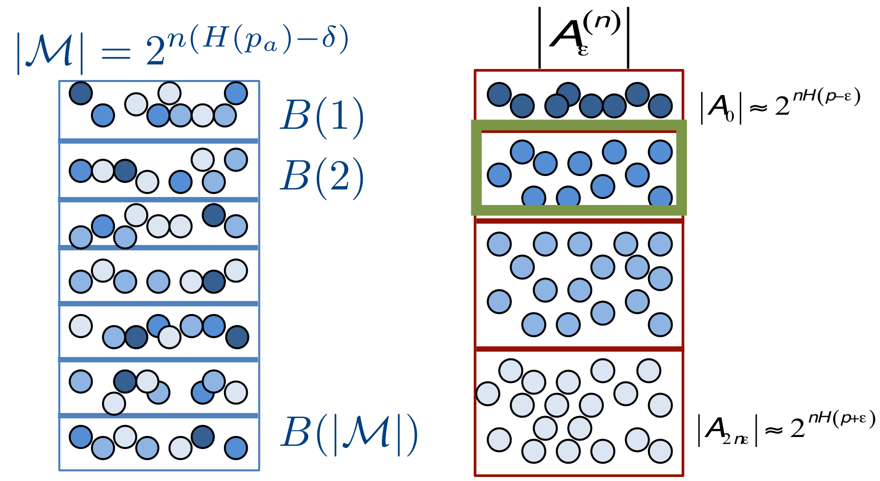




Example: Two links

Attempt 3: Stochastic Encoding

Recall:



Want to show:

$$p_a(B(m)) \to E_{\mathcal{C}}\left[p_a(B(m))\right]$$

$$p_a(B(m)) \approx E_{\mathcal{C}}\left[p_a(B(m))\right](1 \pm \epsilon)$$

$$\boldsymbol{p_a(B(m))} = \sum_{\mathbf{x}\in B(m)} p_a(\mathbf{x})$$

$$= \sum_{T \in \text{ type classes}} \left[\sum_{\mathbf{x}\in T\cap B(m)} p_a(\mathbf{x}) \right]$$

$$= \sum_{T \in \text{ type classes}} \underbrace{|T \cap B(m)|}\ \underbrace{p_{a,T}}$$

sum of i.i.d. terms

constant

Example: Two links

Attempt 3: Stochastic Encoding

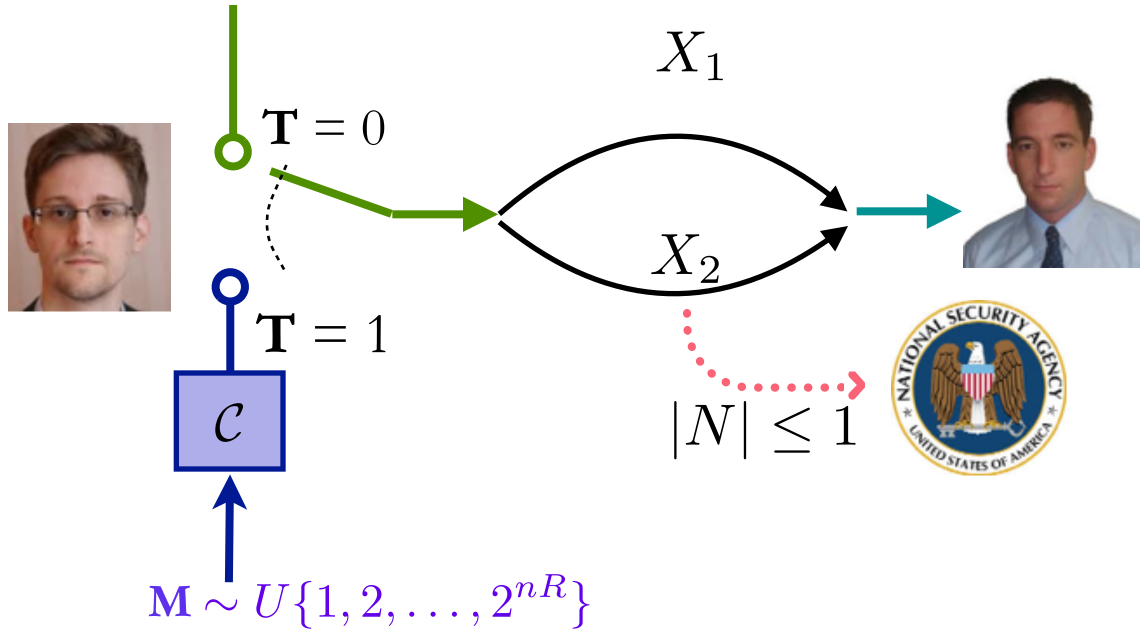
Encoder: $$p(\mathbf{x}|m) = \frac{p_a(\mathbf{x})}{p_a(B(m))} \quad \text{if } \mathbf{x} \in B(m)$$

Shown: $$p_a(B(m)) \rightarrow E_{\mathcal{C}}\left[p_a(B(m))\right]$$ ✓

$$\mathbb{V}(\hat{p}, p_a) = \frac{1}{2}\sum_{\mathbf{x}} |\hat{p}(\mathbf{x}) - p_a(\mathbf{x})|$$

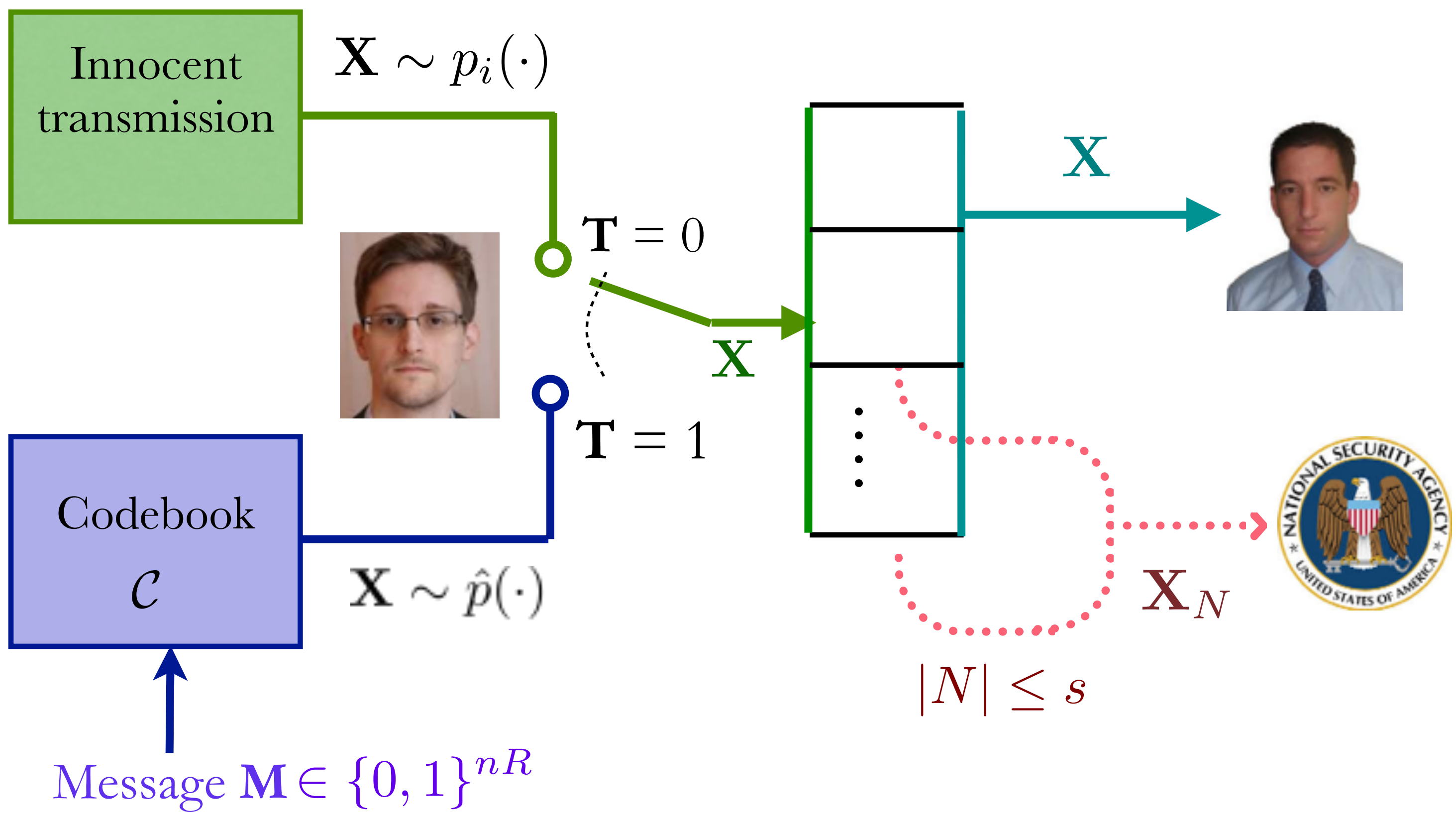
$$< \epsilon/2$$ ✓

Example: Two links



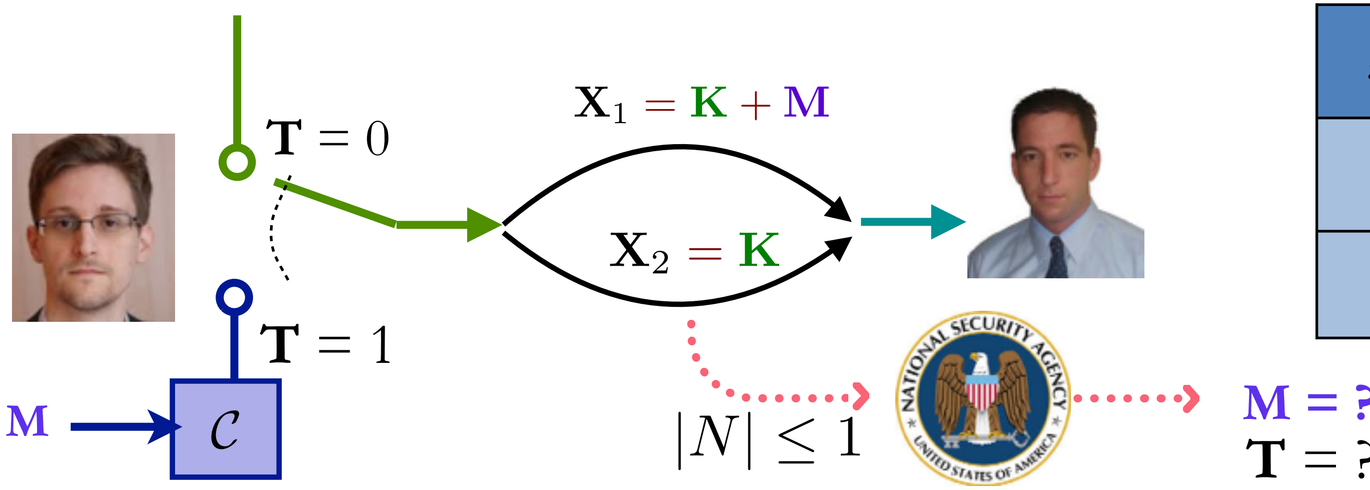
⇒If $R < H_{p_a}(X_1, X_2)$, Reliable and Deniable schemes exist

Network of parallel links



Result: If $R < H_{p_a}(\mathbf{X})$, Reliable and Deniable schemes exist

Hidability (+Deniability)



x_2	
0	***1/3***
1	***2/3***

Q: Can we use standard information theoretic schemes?

e.g.: One-time pad

$\Pr(M = m|\mathbf{X}_i)$ = uniform distribution ⇒ HIDABLE

$\Pr(\mathbf{X}_i)$ also uniform distribution ⇒ NOT DENIABLE

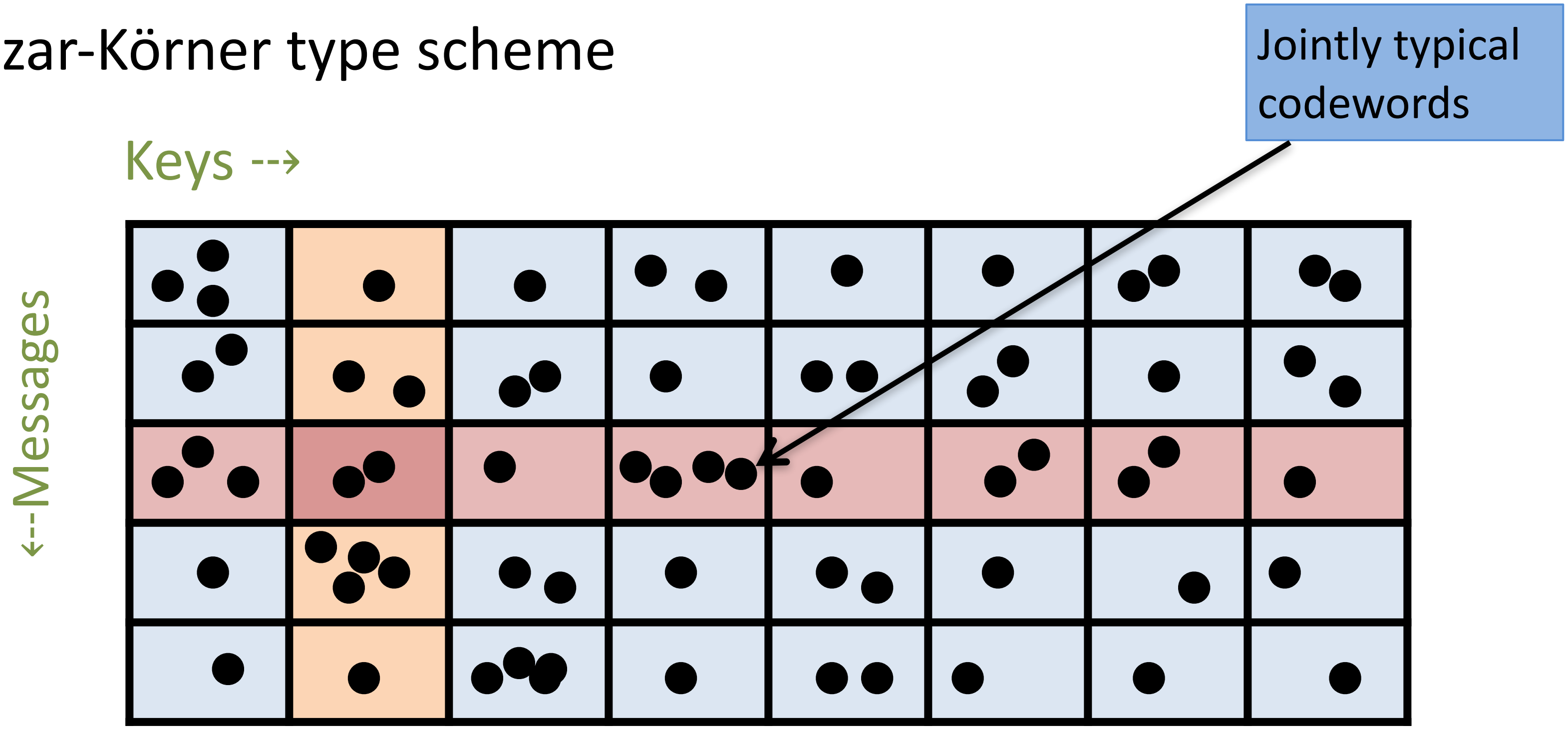
Ideas from converse proof

$$
\begin{aligned}
H(\mathbf{M}) &= H(\mathbf{M}|\mathbf{X}_N) \ \forall |N| \leq s \\
&= H(\mathbf{M}|\mathbf{X}_N) - H(\mathbf{M}|\mathbf{X}_N, \mathbf{X}_{\overline{N}}) + H(\mathbf{M}|\mathbf{X}_N, \mathbf{X}_{\overline{N}}) \\
&\leq H(\mathbf{M}|\mathbf{X}_N) - H(\mathbf{M}|\mathbf{X}_N) + n\epsilon \\
&= I(\mathbf{M}; \mathbf{X}_{\overline{N}}|\mathbf{X}_N) + n\epsilon \\
&= H(\mathbf{X}_{\overline{N}}|\mathbf{X}_N) - H(\mathbf{X}_{\overline{N}}|\mathbf{X}_N, \mathbf{M}) + n\epsilon \\
&\leq H(\mathbf{X}_{\overline{N}}|\mathbf{X}_N) + n\epsilon \\
&\leq \min_{|N| \leq s} H(\mathbf{X}_{\overline{N}}|\mathbf{X}_N) + n\epsilon
\end{aligned}
$$

Random binning?

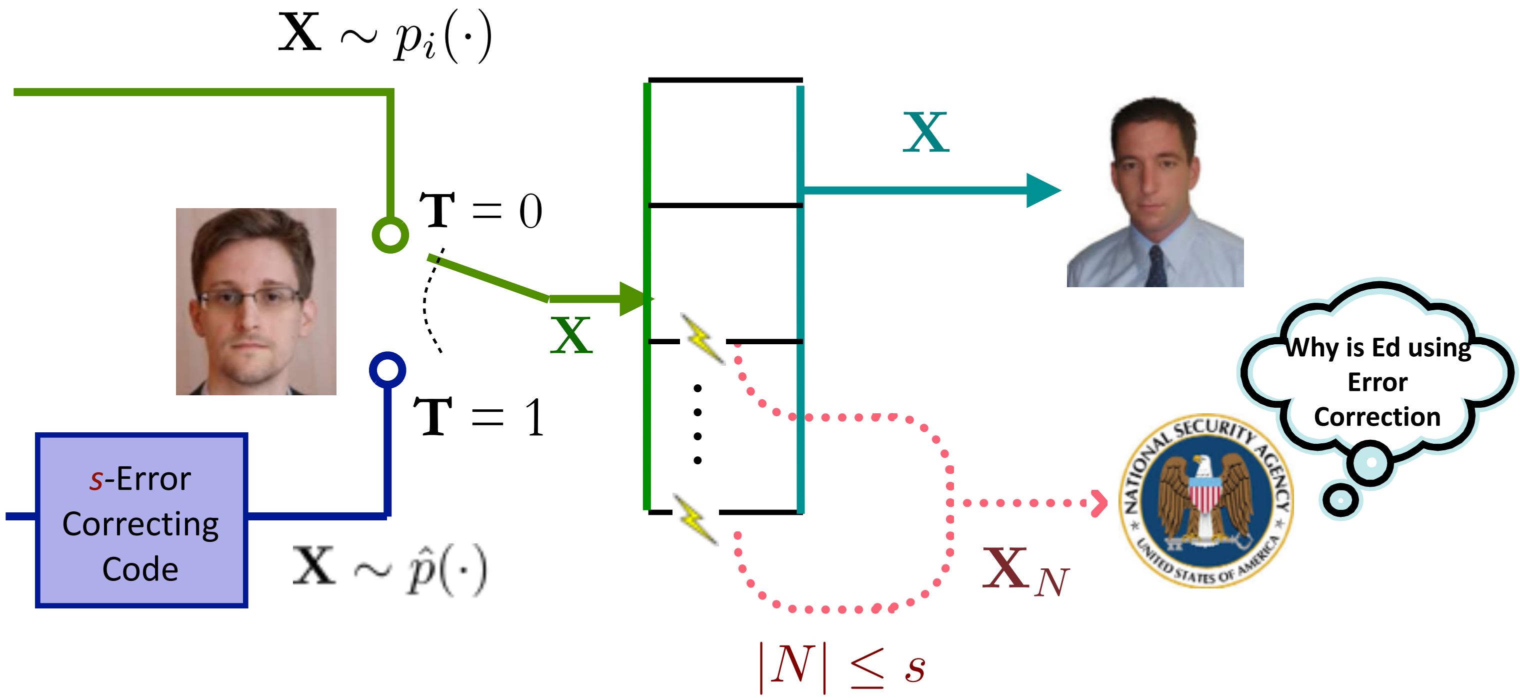
Achievability

Csiszar-Körner type scheme



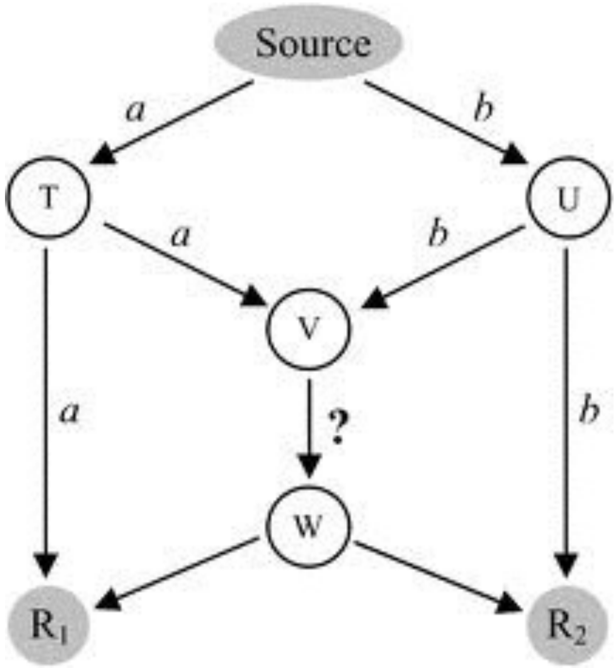
[2] I. Csiszár and J. Körner, "Broadcast channels with confidential messages," IEEE Transactions on Information Theory, vol. 24, pp. 339–348, May 1978.

Correctability (+Deniability)



Q: Can we use off the shelf network error correction codes?

Deniability over Networks

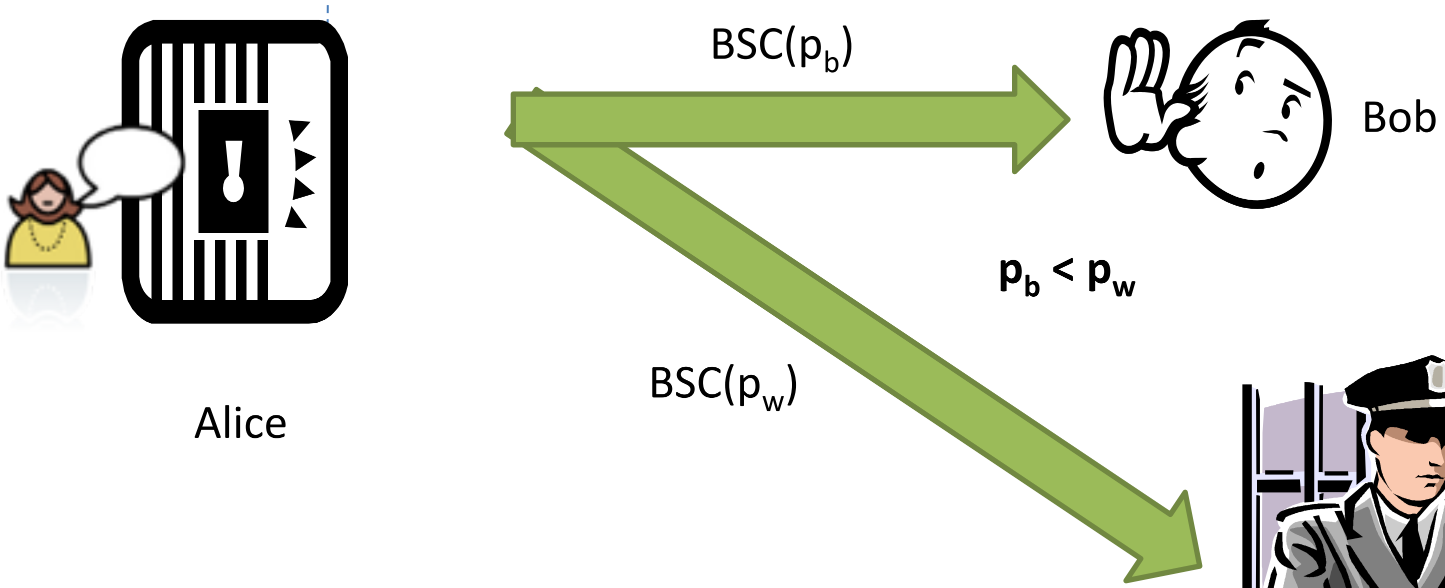


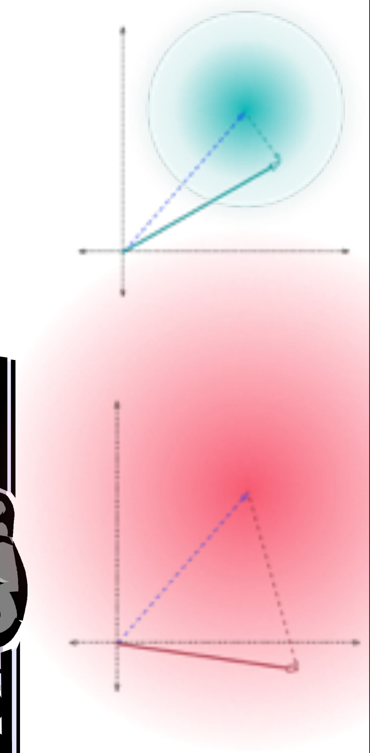
Q: How would coding at intermediate nodes affect the deniability?

— Malicious nodes?

…

Trick 2: Hiding in noise

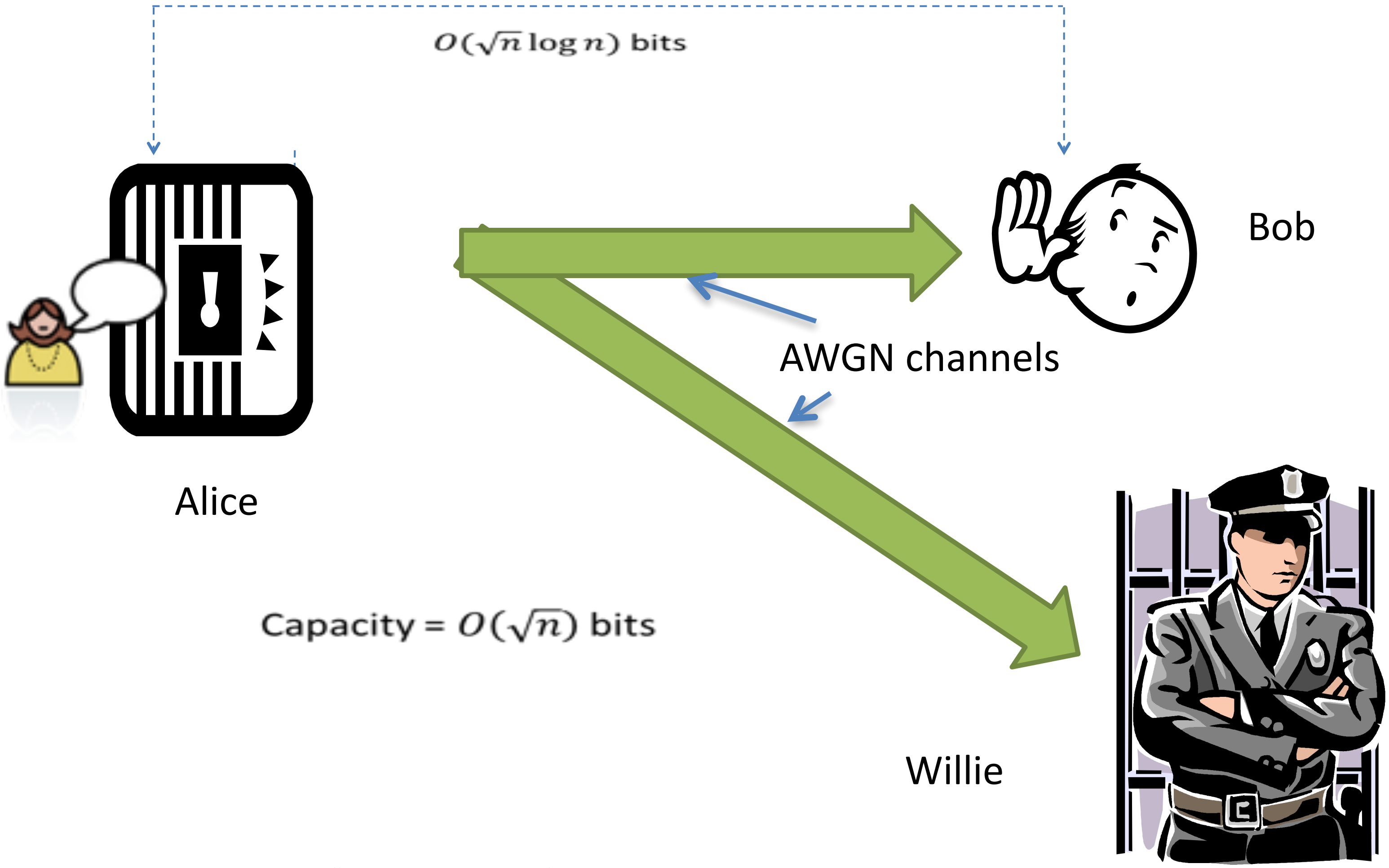




Innocent transmission = all 0's

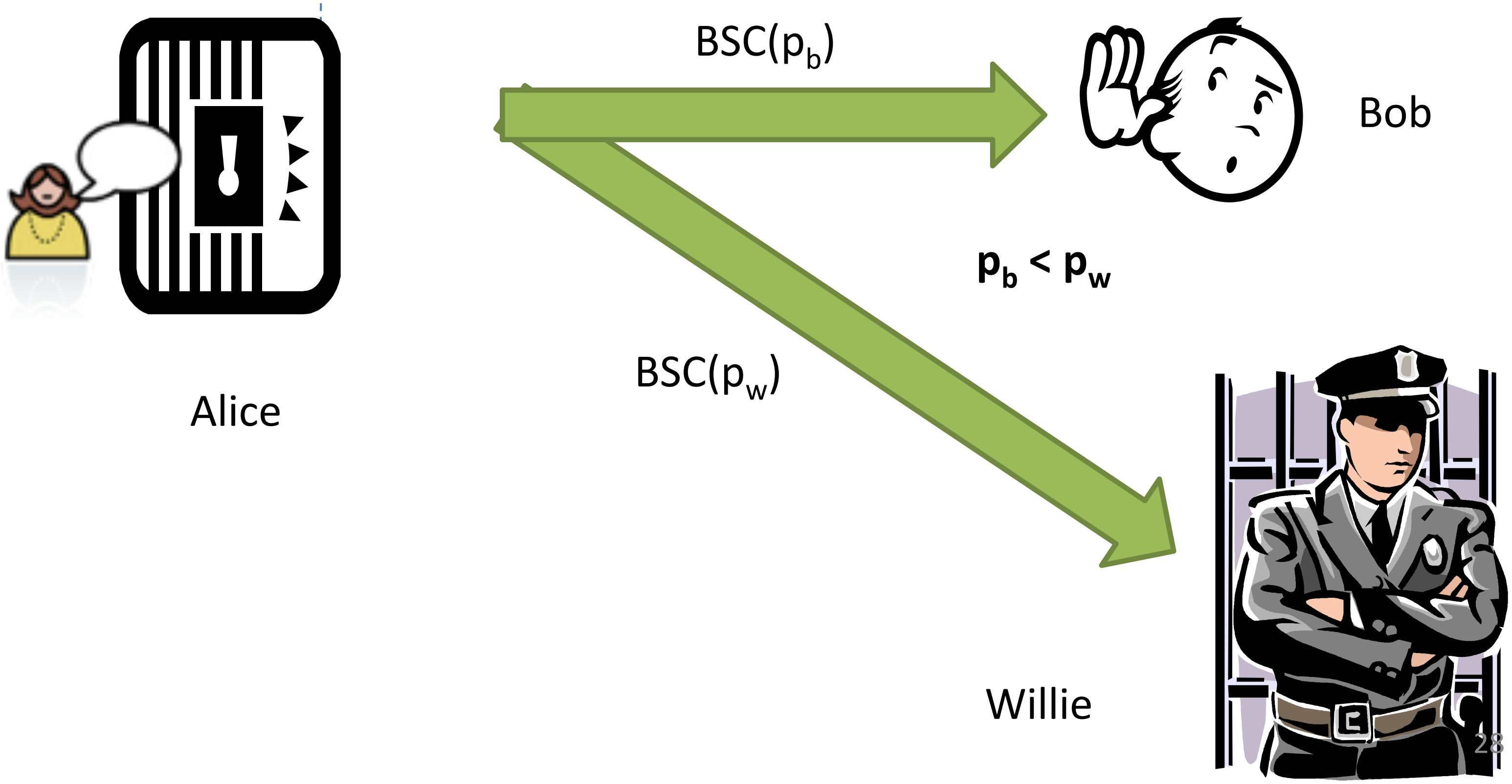
Capacity = $O(1/\sqrt{n})$

Prior work: shared secret



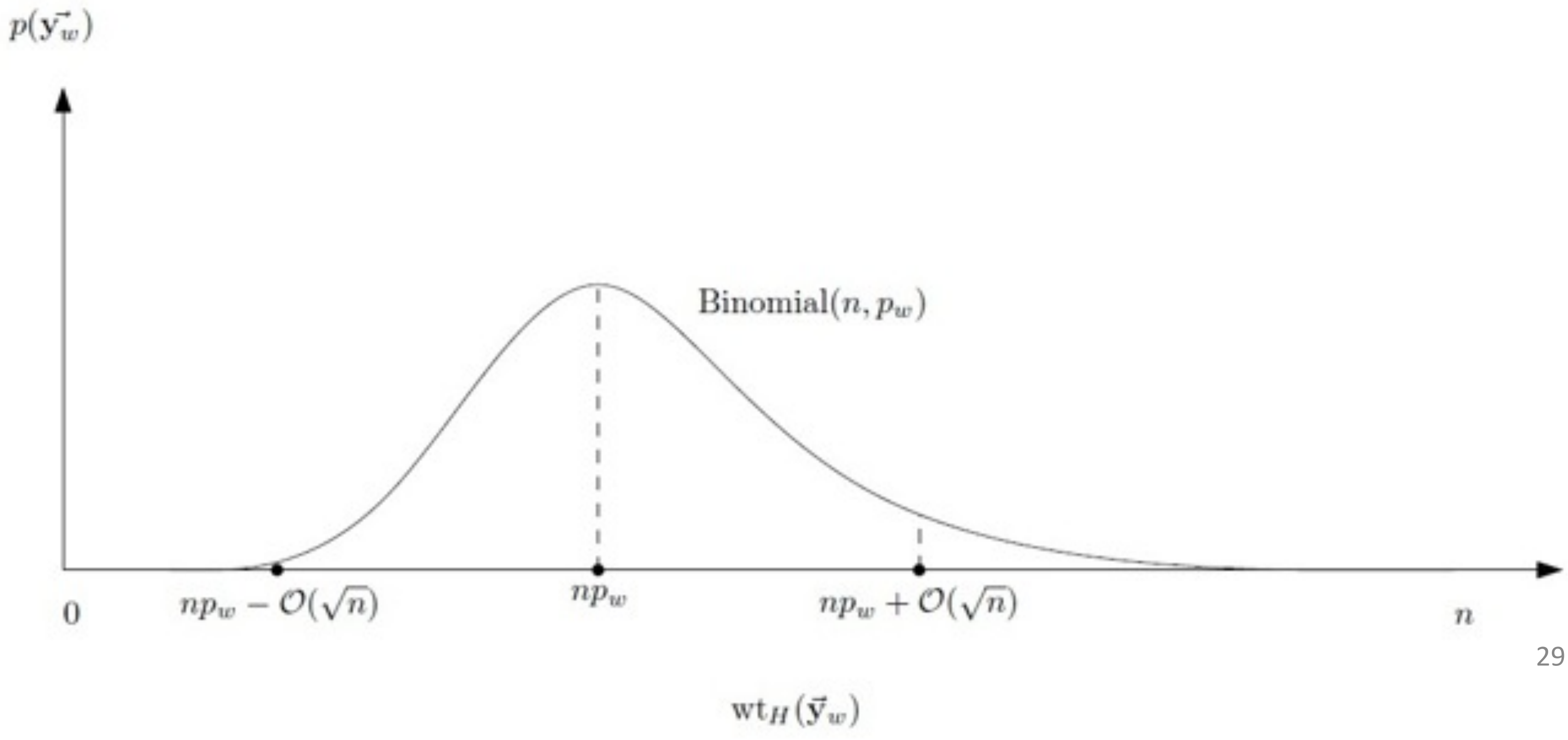
[1] B. A. Bash, D. Goeckel and D. Towsley, "Square root law for communication with low probability of detection on AWGN channels," *in Proceedings of the IEEE International Symposium on Information Theory (ISIT)*, 2012, pp. 448–452.

Our work: no shared secret [ISIT'13]



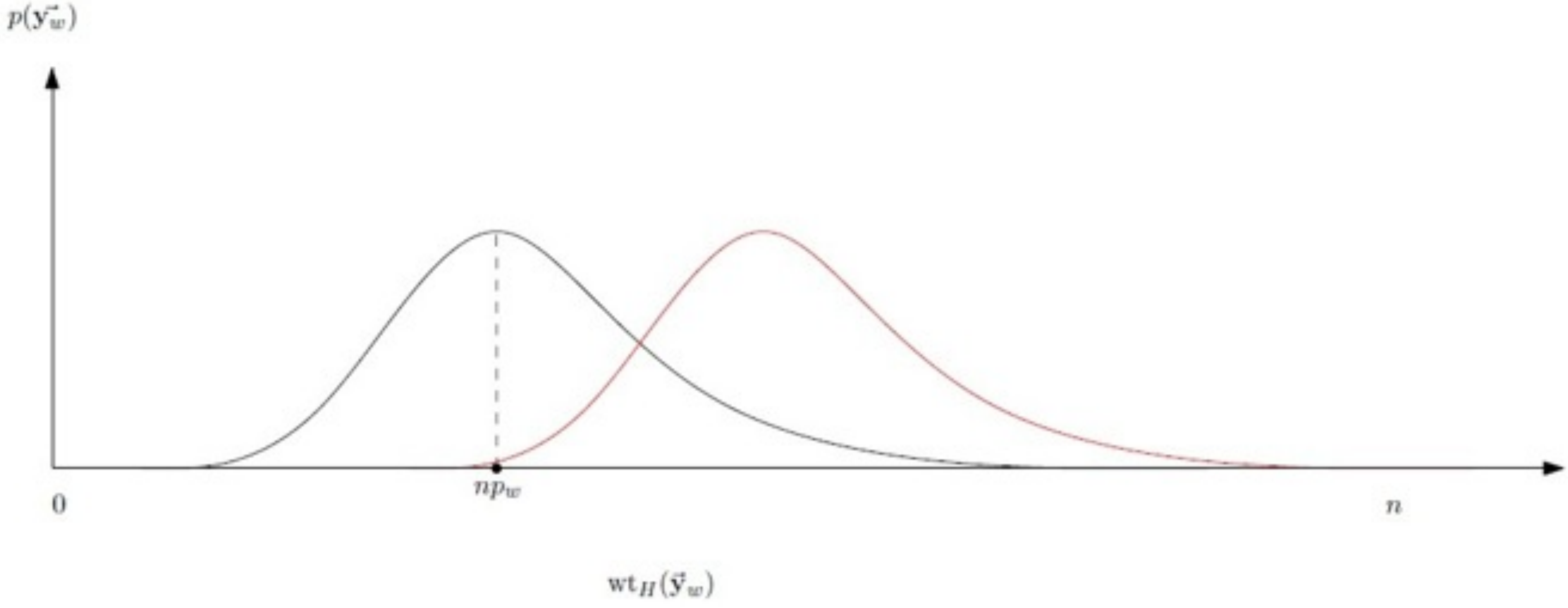
Intuition: How loudly can Alice whisper?

- $\mathbf{T} = 0, \vec{\mathbf{y}}_w = \vec{\mathbf{z}}_w \sim \text{Binomial}(n, p_w)$



Intuition: How loudly can Alice whisper?

- $\mathbf{T} = 0, \vec{\mathbf{y}}_w = \vec{\mathbf{z}}_w \sim \text{Binomial}(n, p_w)$
- $When\ \mathbf{T} = 1,$

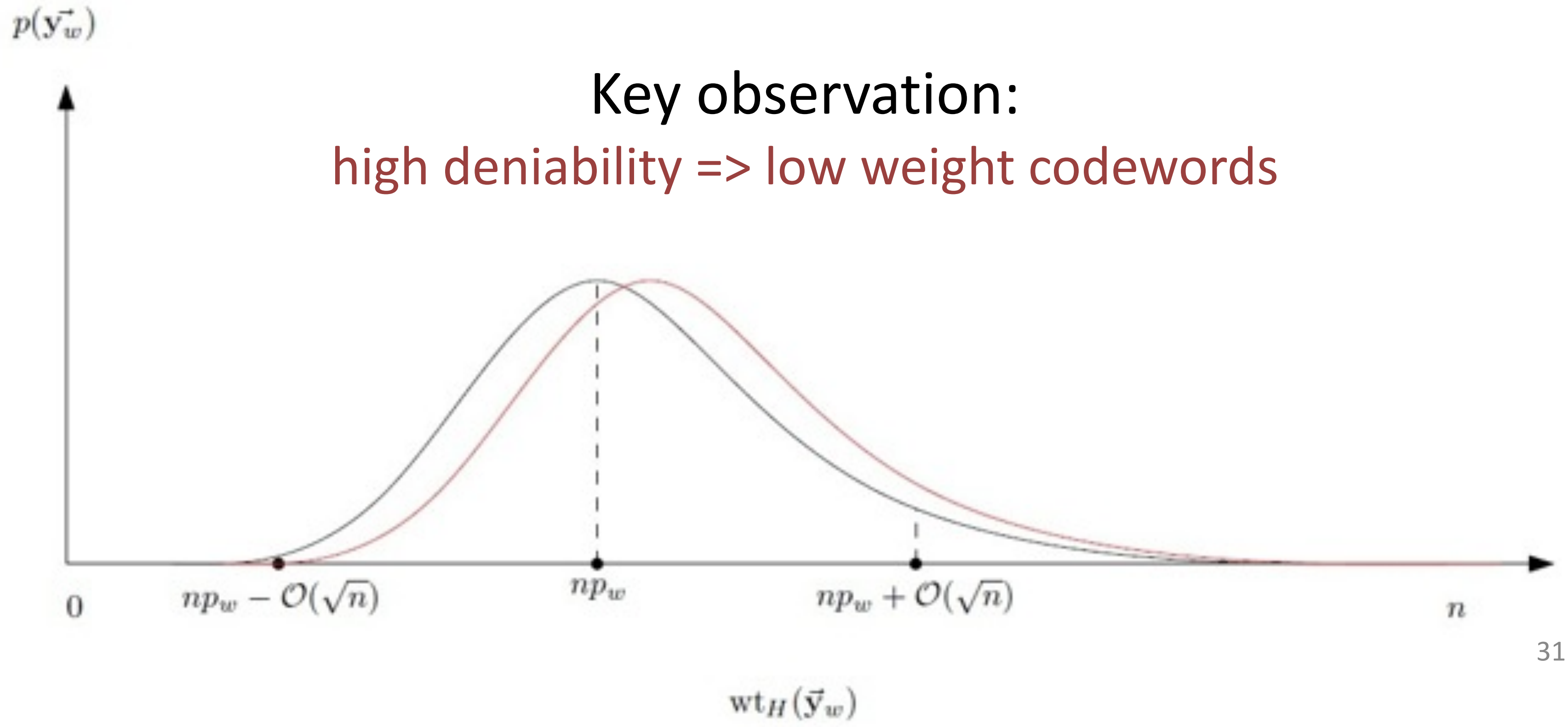


Intuition: How loudly can Alice whisper?

- $\mathbf{T} = 0, \vec{\mathbf{y}}_w = \vec{\mathbf{z}}_w \sim \text{Binomial}(n, p_w)$
- $When\ \mathbf{T} = 1,$

Key observation:

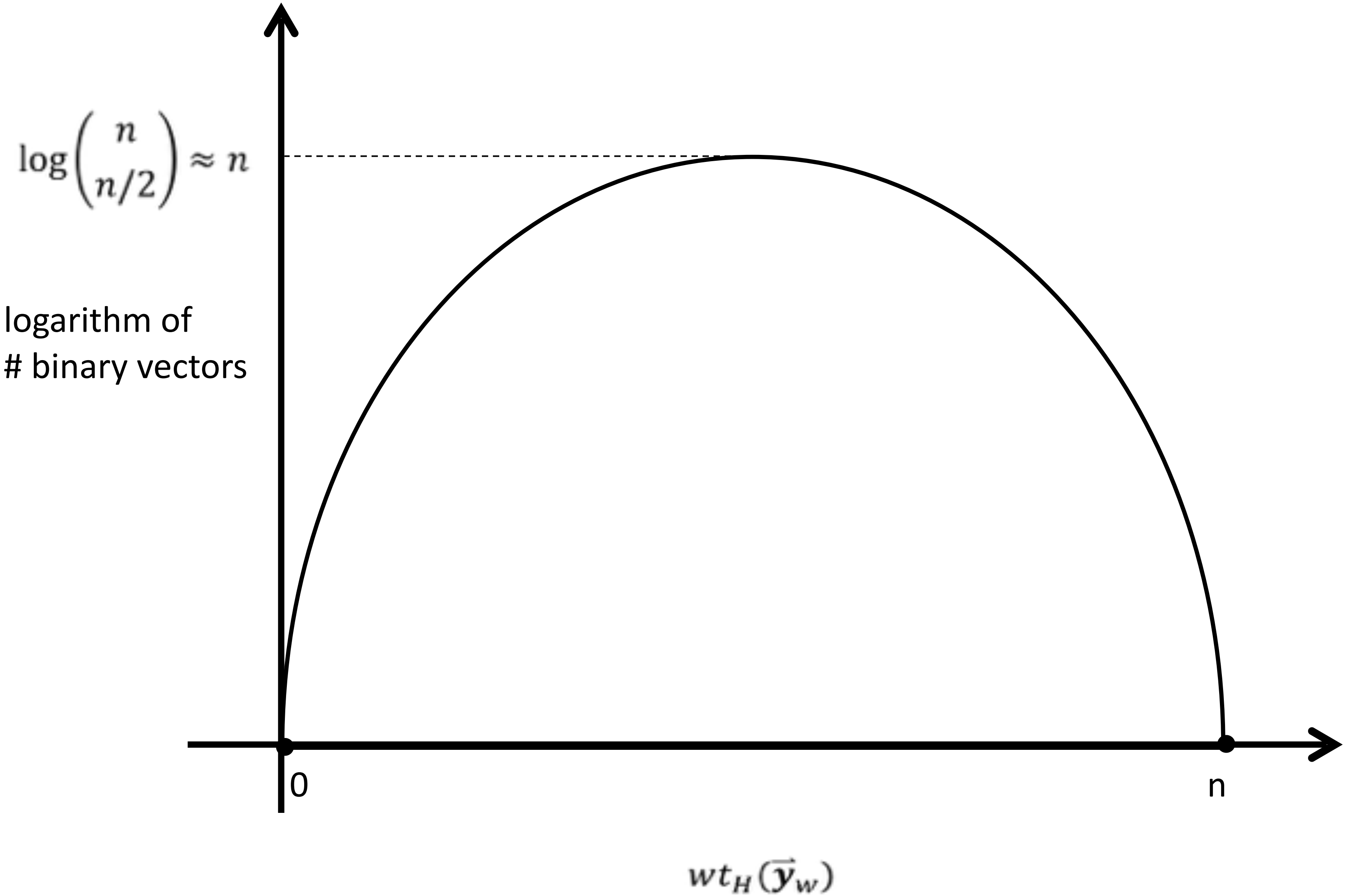
high deniability => low weight codewords



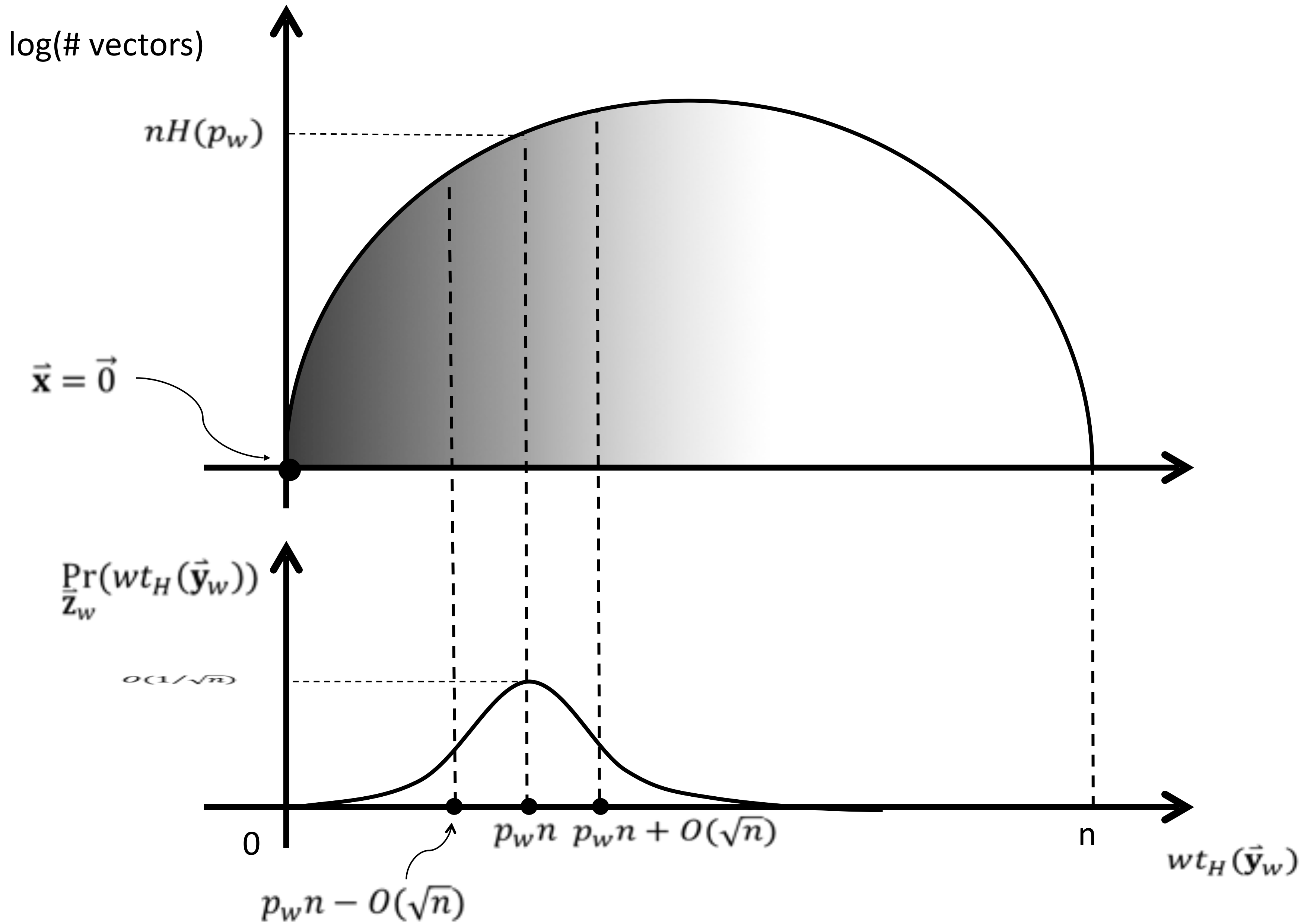
Reliability

- Random codebook (i.i.d. $\rho = O(1/\sqrt{n})$)
- minimum distance decoder

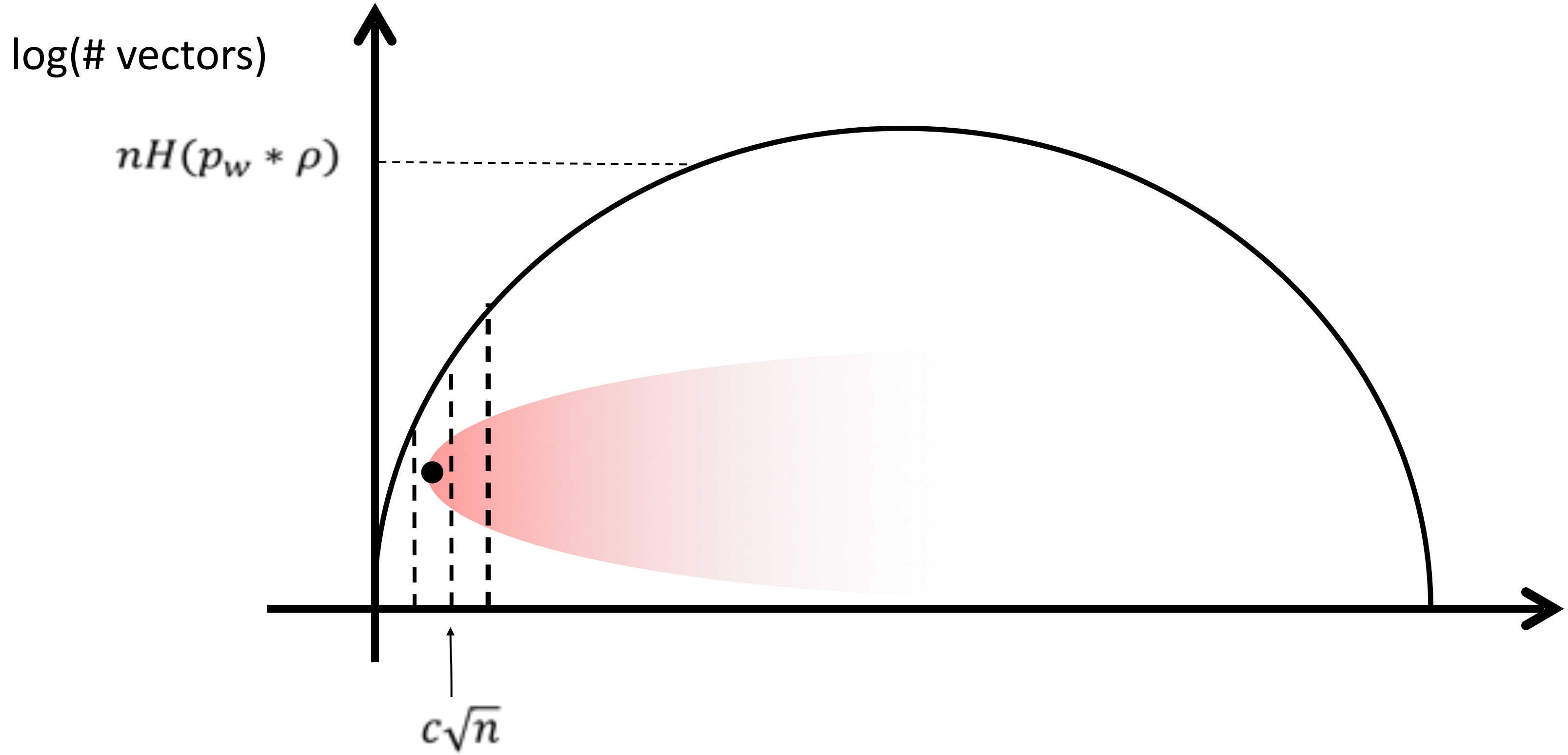
Rate = $O(1/\sqrt{n}) \implies \Pr(\text{error}) \to 0$

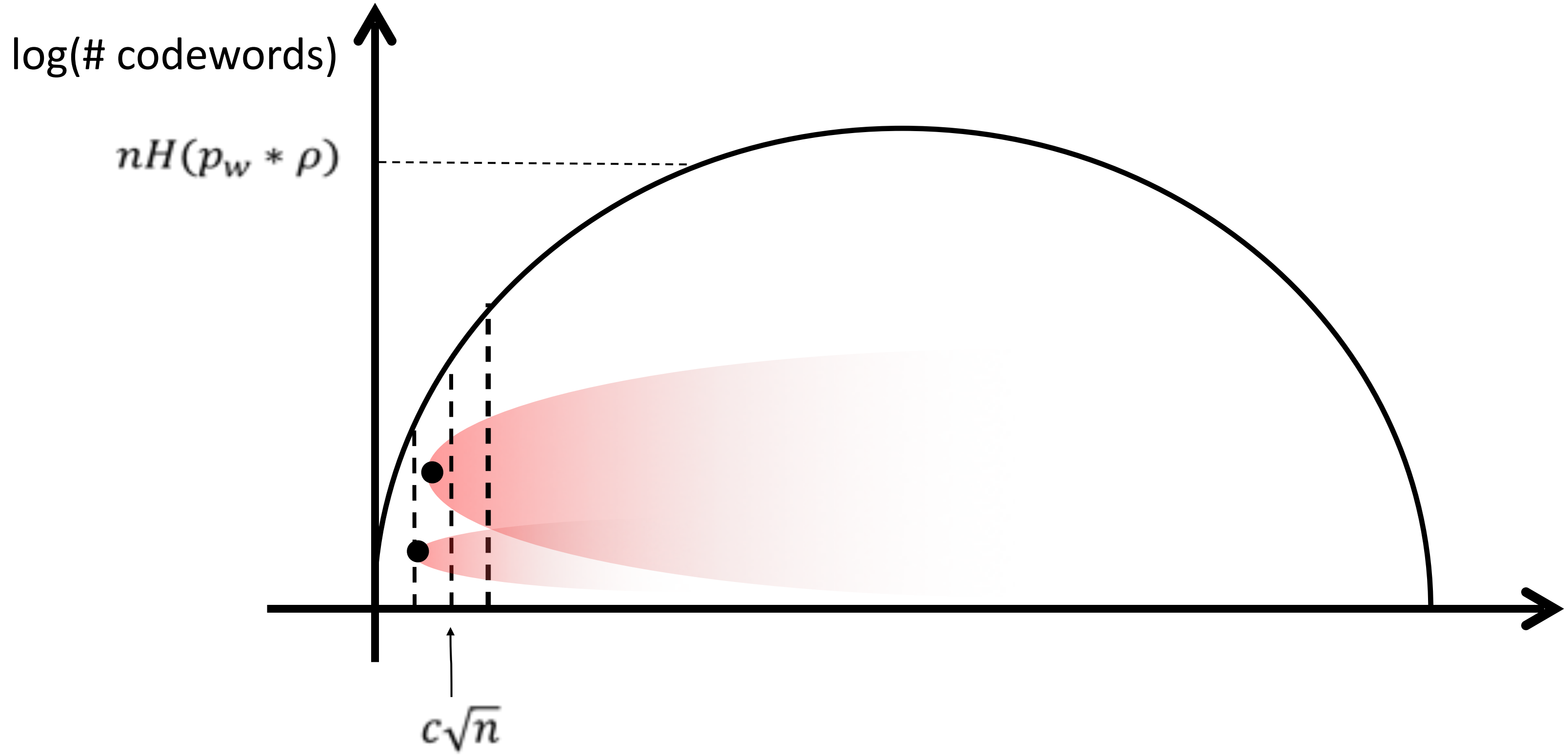


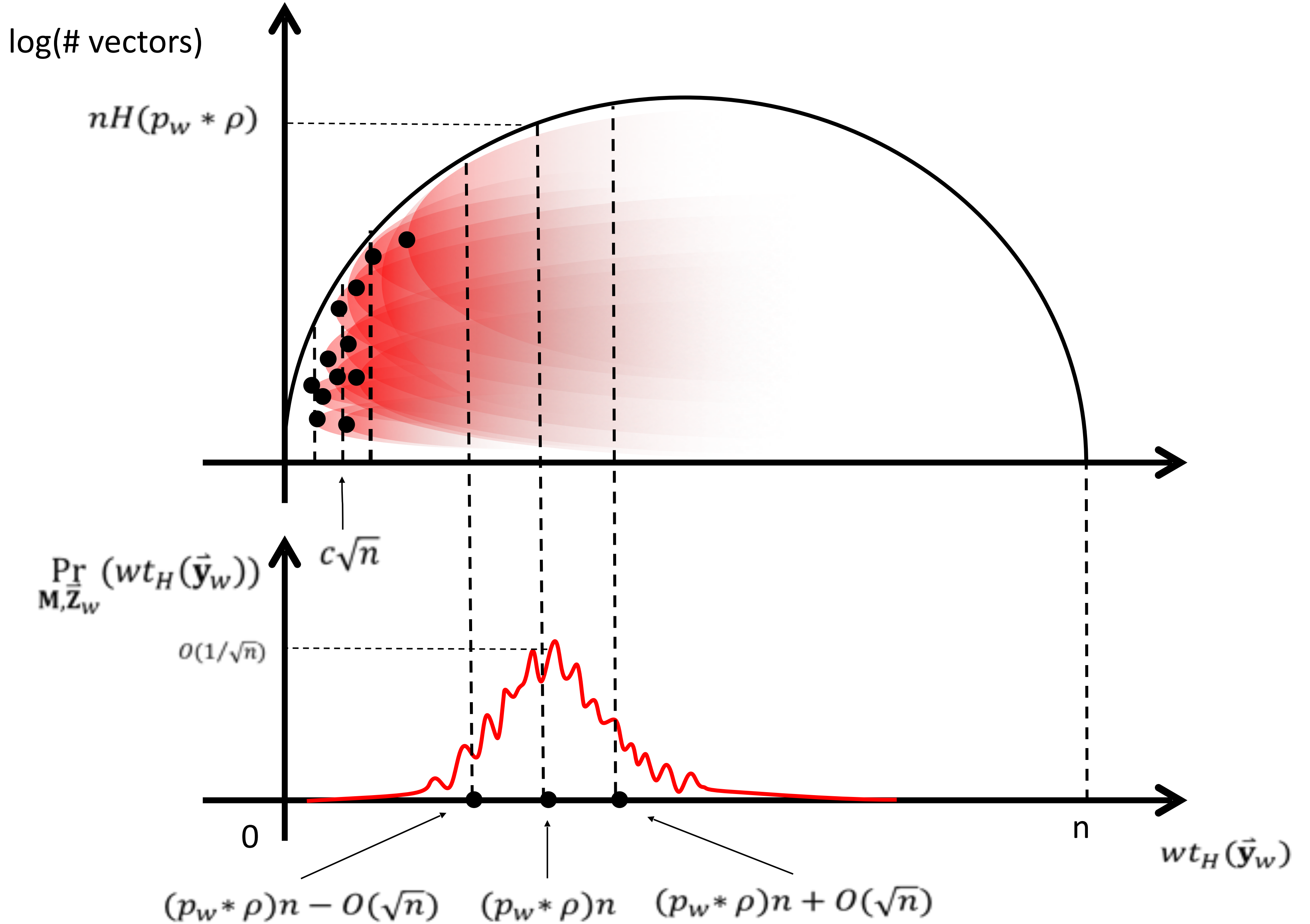
$\log\binom{n}{n/2} \approx n$
logarithm of
binary vectors
0
n
$wt_H(\vec{y}_w)$



log(# vectors)
$nH(p_w)$
$\vec{\mathbf{x}} = \vec{0}$
$\Pr_{\vec{\mathbf{z}}_w}(wt_H(\vec{\mathbf{y}}_w))$
$O(1/\sqrt{n})$
0
$p_w n$
$p_w n + O(\sqrt{n})$
n
$wt_H(\vec{\mathbf{y}}_w)$
$p_w n - O(\sqrt{n})$


log(# vectors)
$nH(p_w * \rho)$
$c\sqrt{n}$

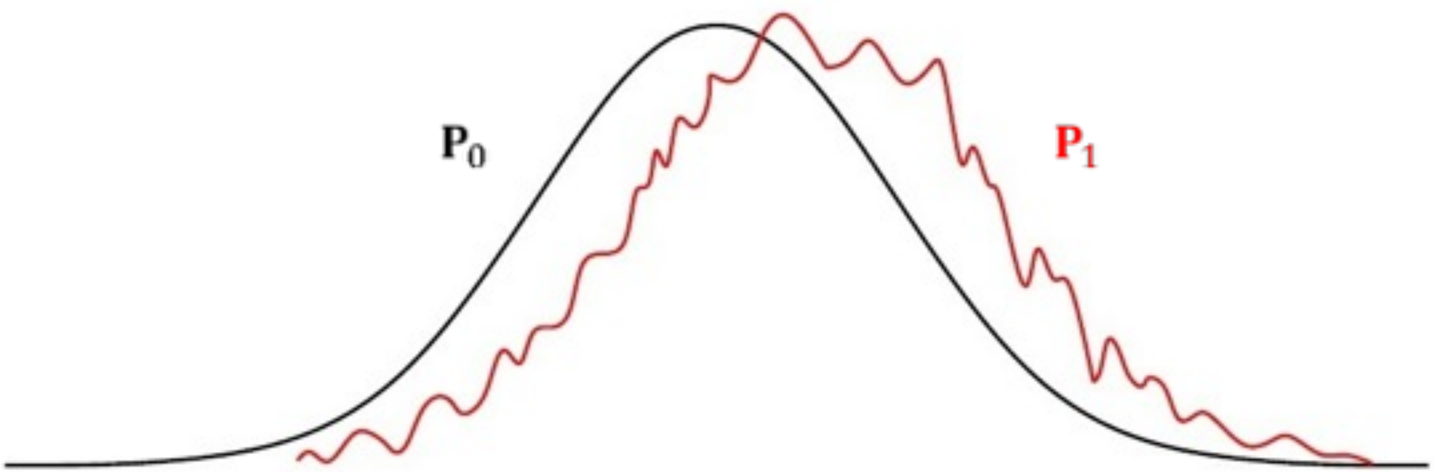

log(# codewords)
$nH(p_w * \rho)$
$c\sqrt{n}$



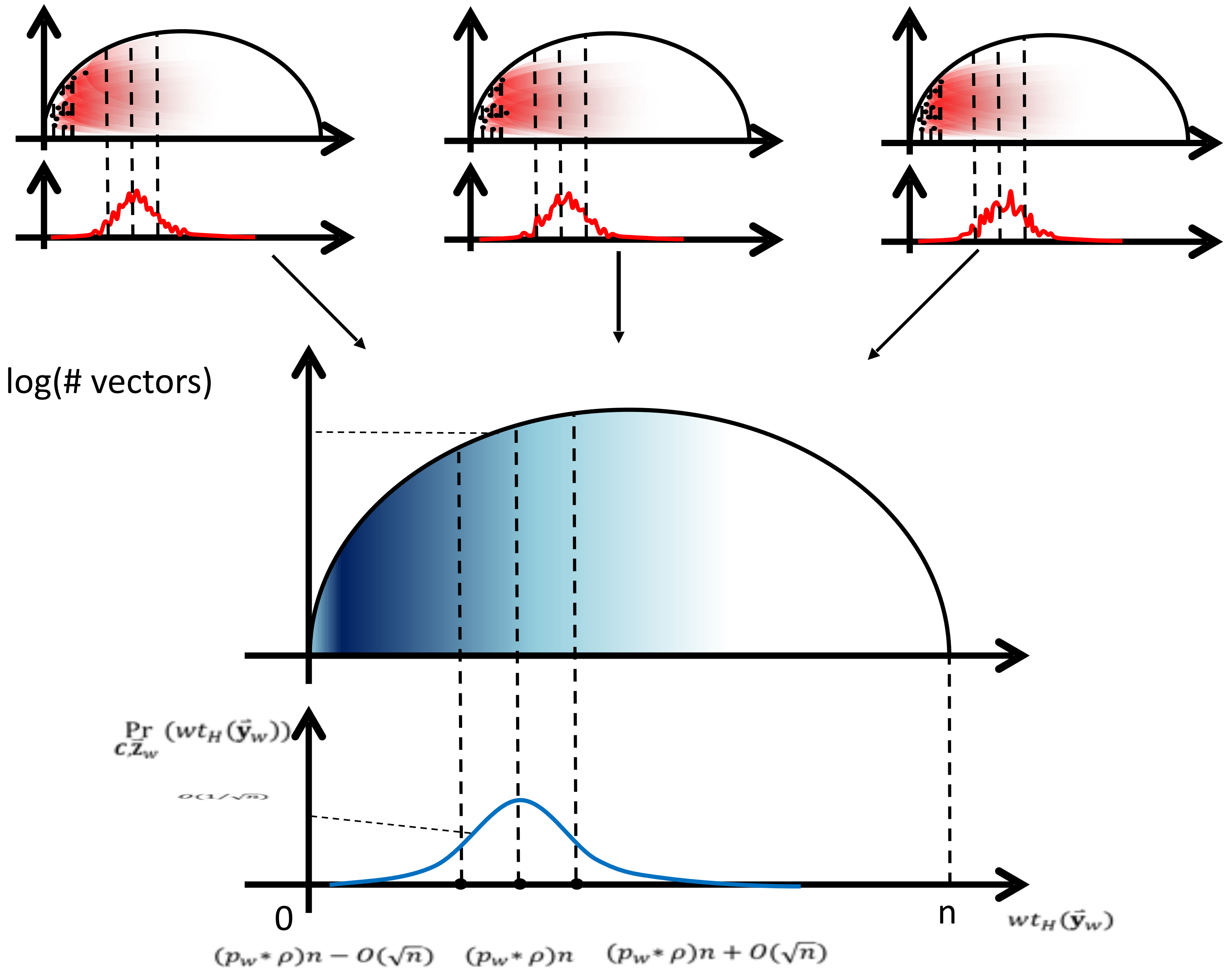
log(# vectors)
$nH(p_w * \rho)$
$c\sqrt{n}$
$\Pr_{\mathbf{M},\vec{\mathbf{Z}}_w}(wt_H(\vec{\mathbf{y}}_w))$
$O(1/\sqrt{n})$
0
n
$wt_H(\vec{\mathbf{y}}_w)$
$(p_w * \rho)n - O(\sqrt{n})$
$(p_w * \rho)n$
$(p_w * \rho)n + O(\sqrt{n})$

Deniability proof sketch

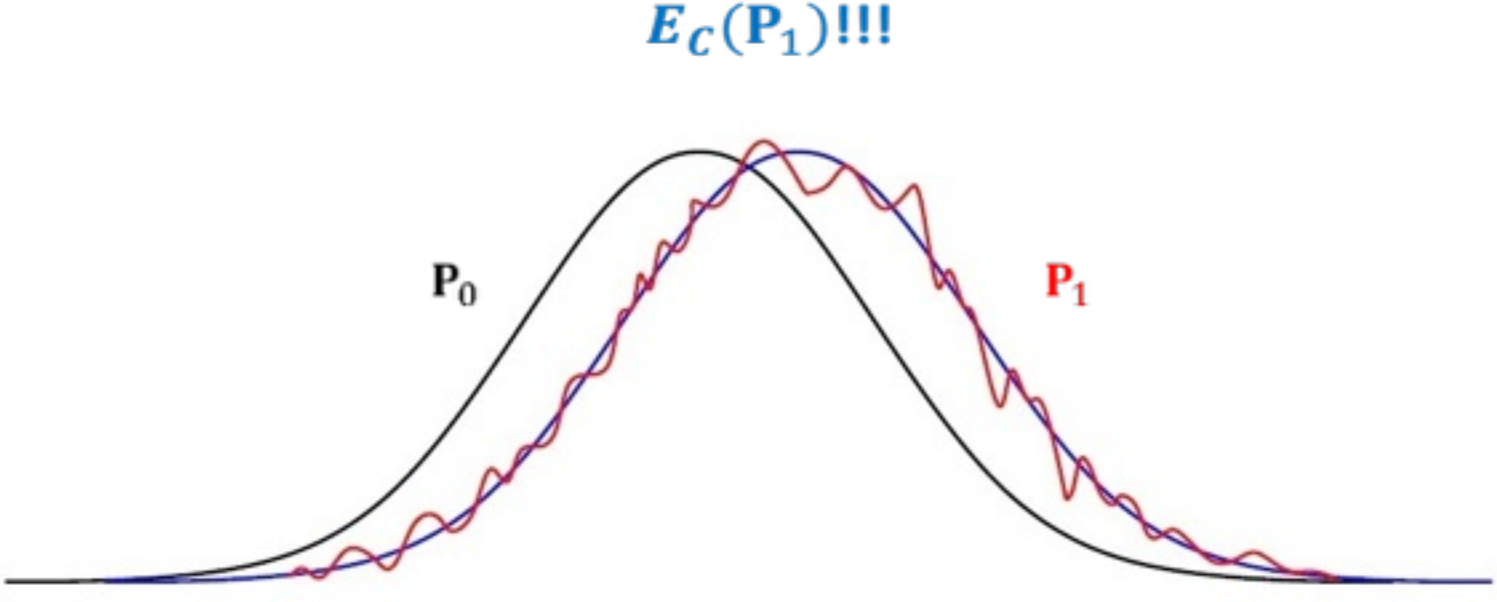
- Recall: want to show $\Pr(V(\mathbf{P}_0, \mathbf{P}_1) < \epsilon) > 1 - \delta$



Deniability proof sketch



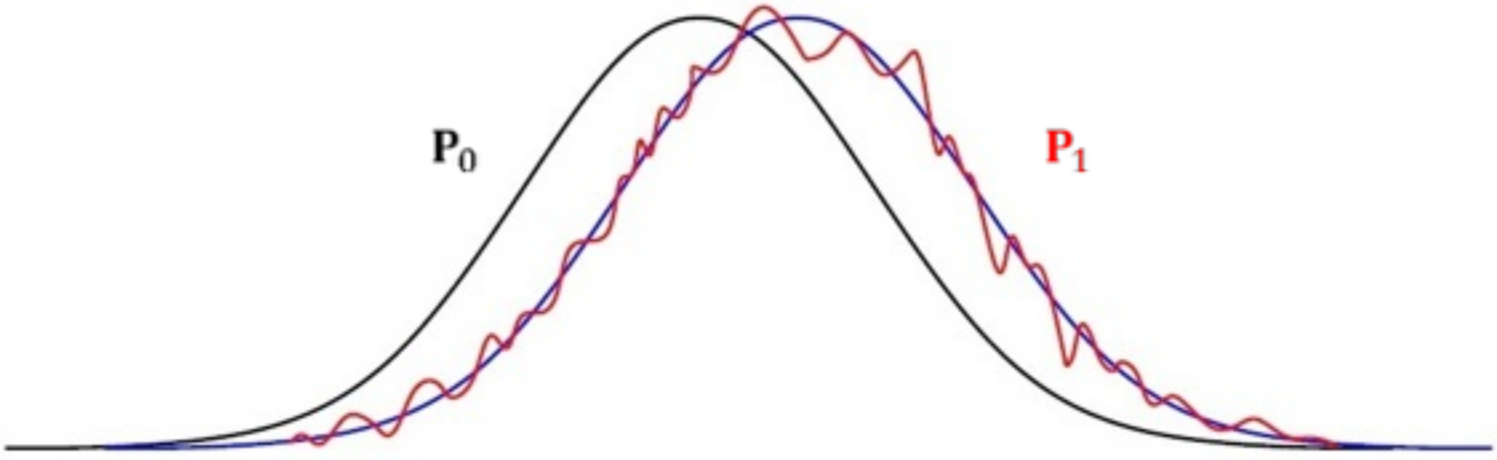
Deniability proof sketch



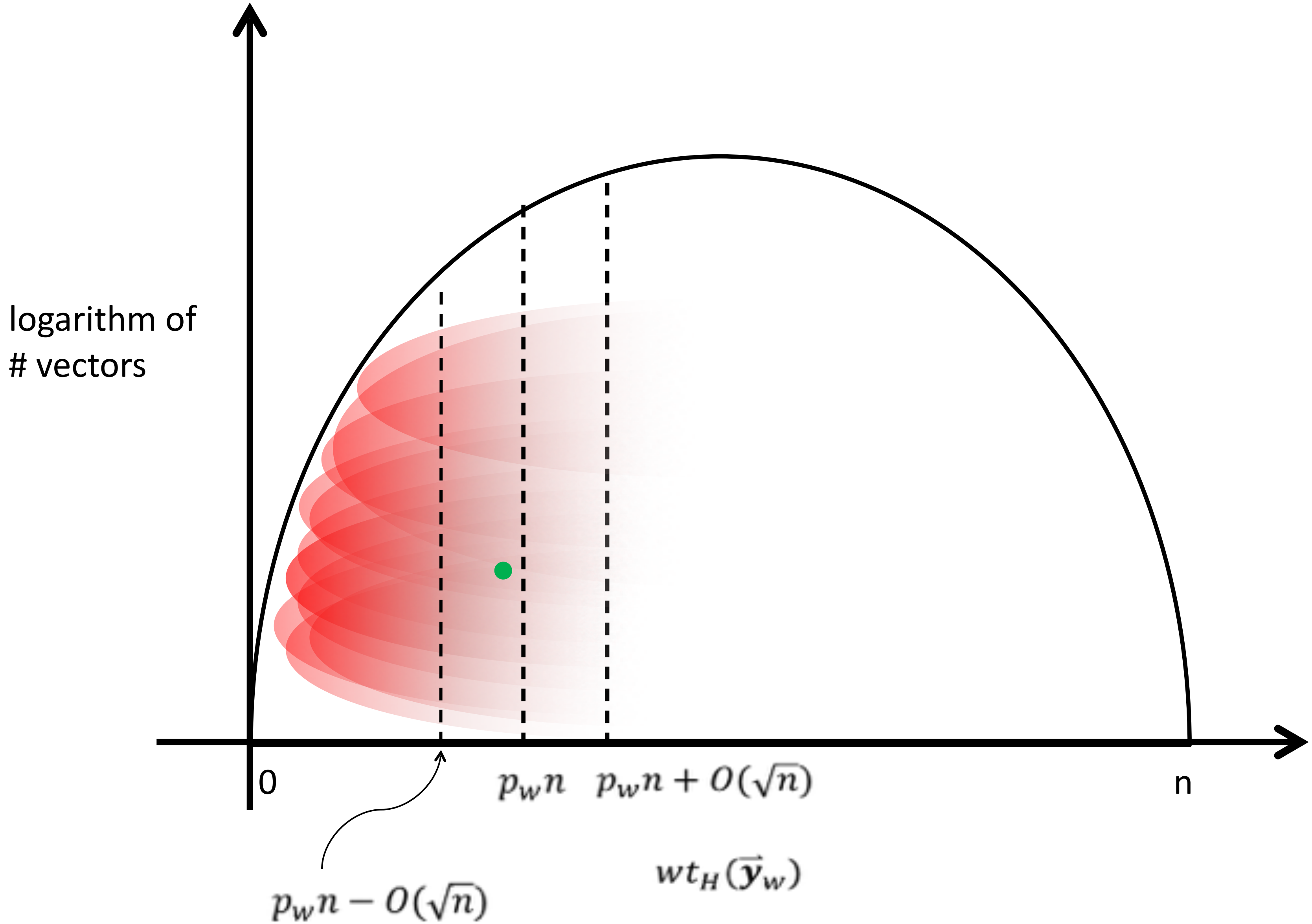
Deniability proof sketch

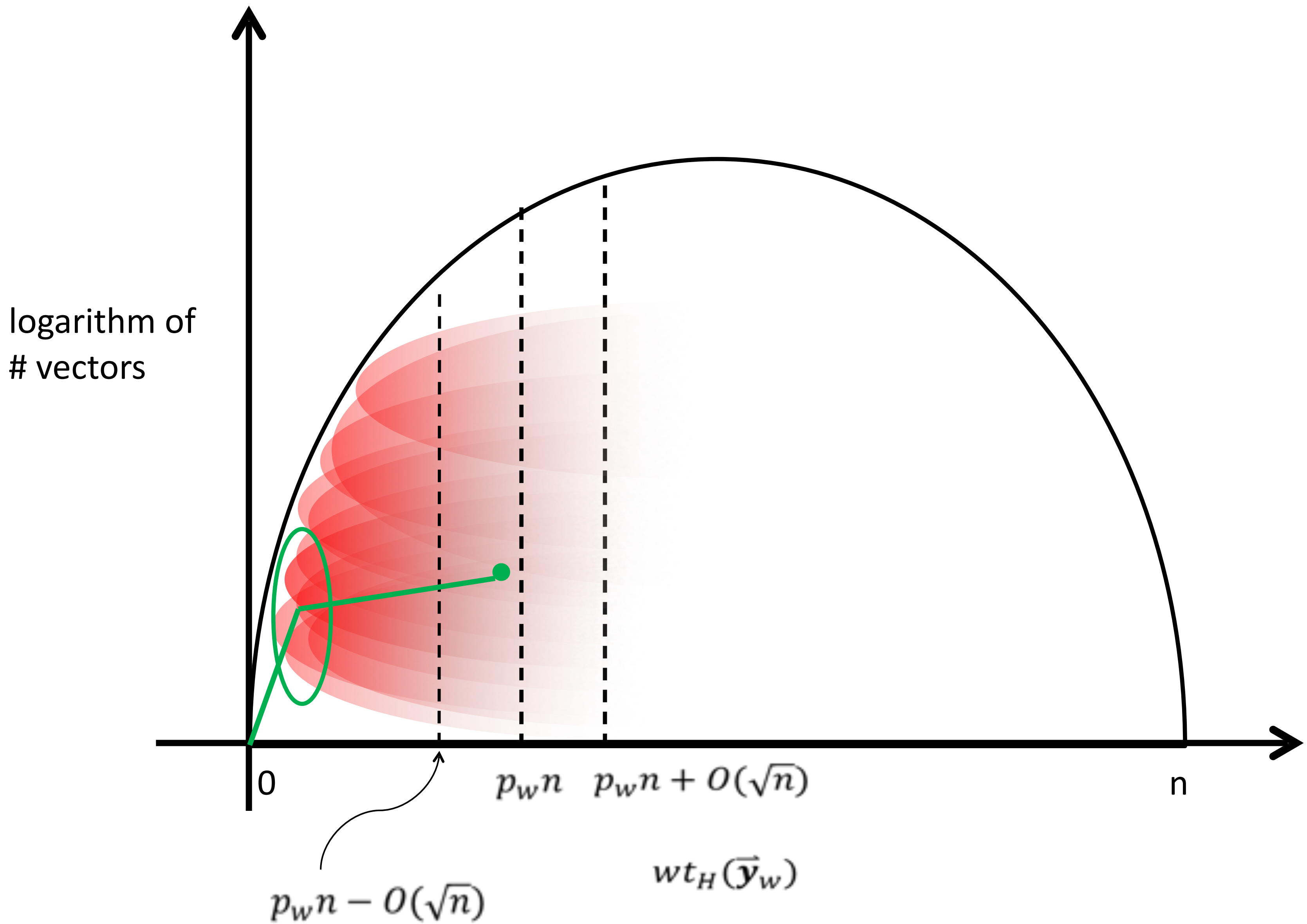
- $V(\mathbf{P}_0, \mathbf{P}_1) \leq V(\mathbf{P}_0, \boldsymbol{E_C}(\mathbf{P}_1)) + V(\boldsymbol{E_C}(\mathbf{P}_1), \mathbf{P}_1)$

$\boldsymbol{E_C}(\mathbf{P}_1)$!!!



Deniability proof sketch




logarithm of
vectors
0
$p_w n$
$p_w n + O(\sqrt{n})$
n
$wt_H(\vec{\boldsymbol{y}}_w)$
$p_w n - O(\sqrt{n})$

Conclusion

Deniability

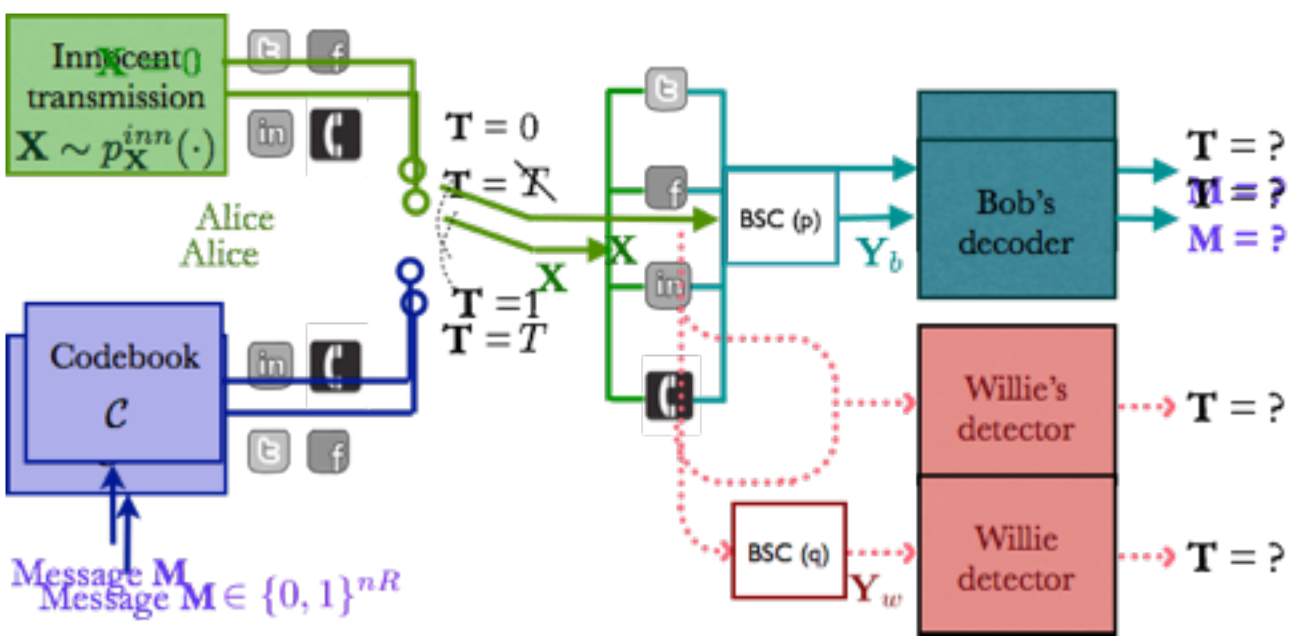
- a new notion of information theoretic security
- fundamentally information theoretic ?

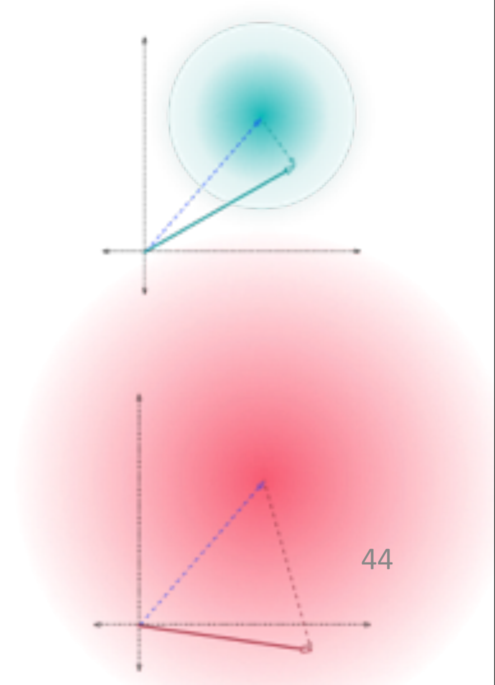
Hidability

- "Super-strong secrecy" : stronger notion than strong secrecy
- Deniability + Hidability

Pretending Innocence

Hiding in noise





Many unsolved problems

General Networks

Deniability + other metrics (correctibility, anonymity, …)

Leveraging other asymmetries

- channel uncertainty
- shared randomness

Interactive communication

Computational deniability (pseudorandomness…)

Other Research Themes

Arbitrary Varying Channels

Farzin Haddadpour, Mahdi Jafari Siavoshani, Sid Jaggi [ISIT'13]

Adaptive Network Coding

[Invited talk BIRS'13]

Network Convolutional Codes/Network Codes and Control Systems

Jithin R, Zitan Chen, Sid Jaggi

Joint Source-Channel Codes for Broadcast

Qiwen Wang, Sid Jaggi

Network Tomography/Compressive Sensing/Group Testing/Phase Recovery

Sheng Cai, Eric Chan, Minghua Chen, Sid Jaggi

[Allerton'12, ITW'13, Allerton'13, COMSNETS'14]

Other “Fun” Stuff

Grant proposals (with Prof Sid Jaggi)

2 GRF grants, Google grants

Teaching

Course material, help with teaching…

“Community service”

2 TPCs, journal reviews, Network Coding website etc

Fun activities

CAN-DO-IT poster day, help with workshops

Thank You!