

# Saddle-point Solution of the Fingerprinting Capacity Game Under the Marking Assumption

Yen-Wei Huang, Pierre Moulin

Beckman Inst., Coord. Sci. Lab and ECE Department, University of Illinois at Urbana-Champaign

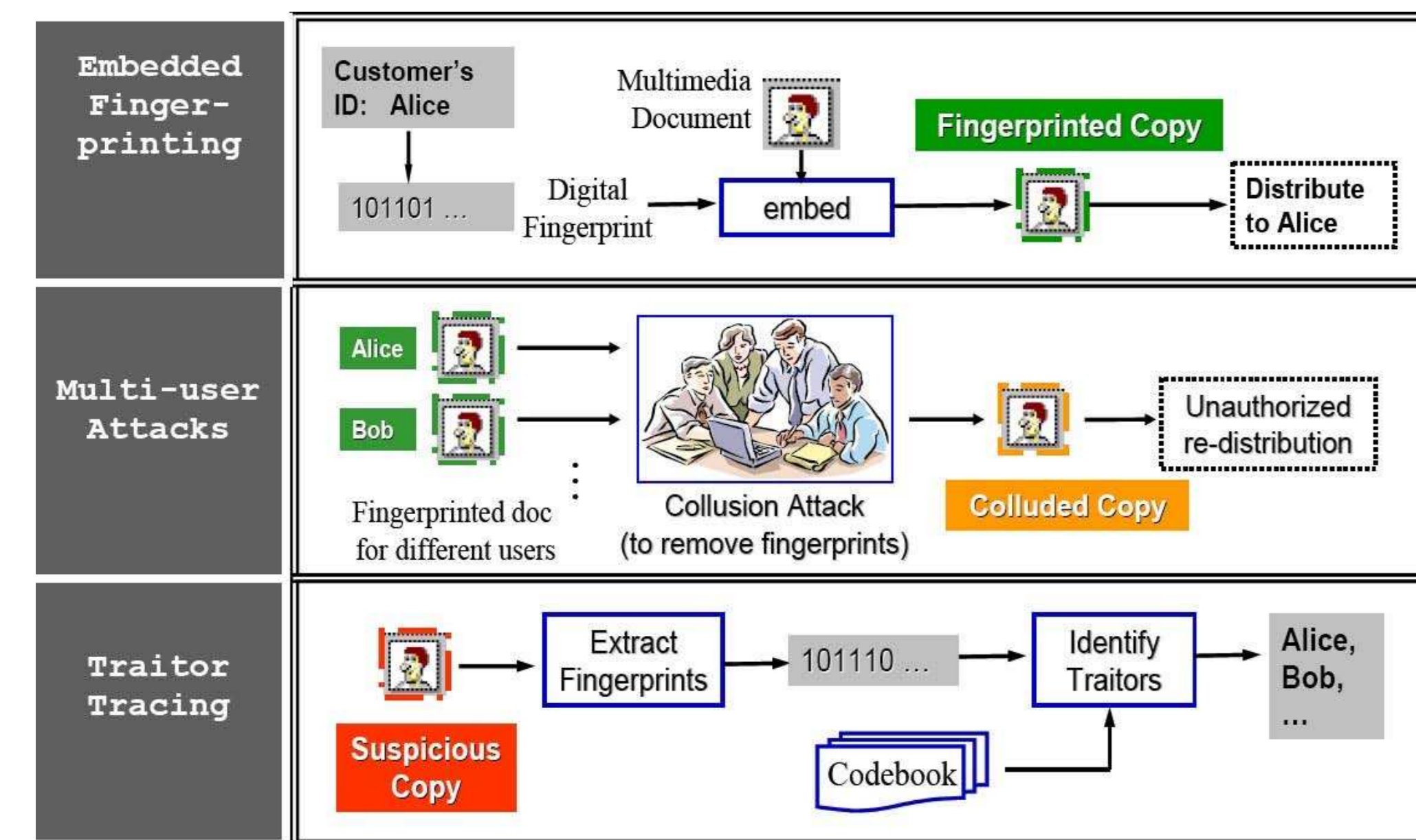
Email: huang37@illinois.edu, moulin@ifp.uiuc.edu



## What is Fingerprinting?

### Fingerprinting System Overview

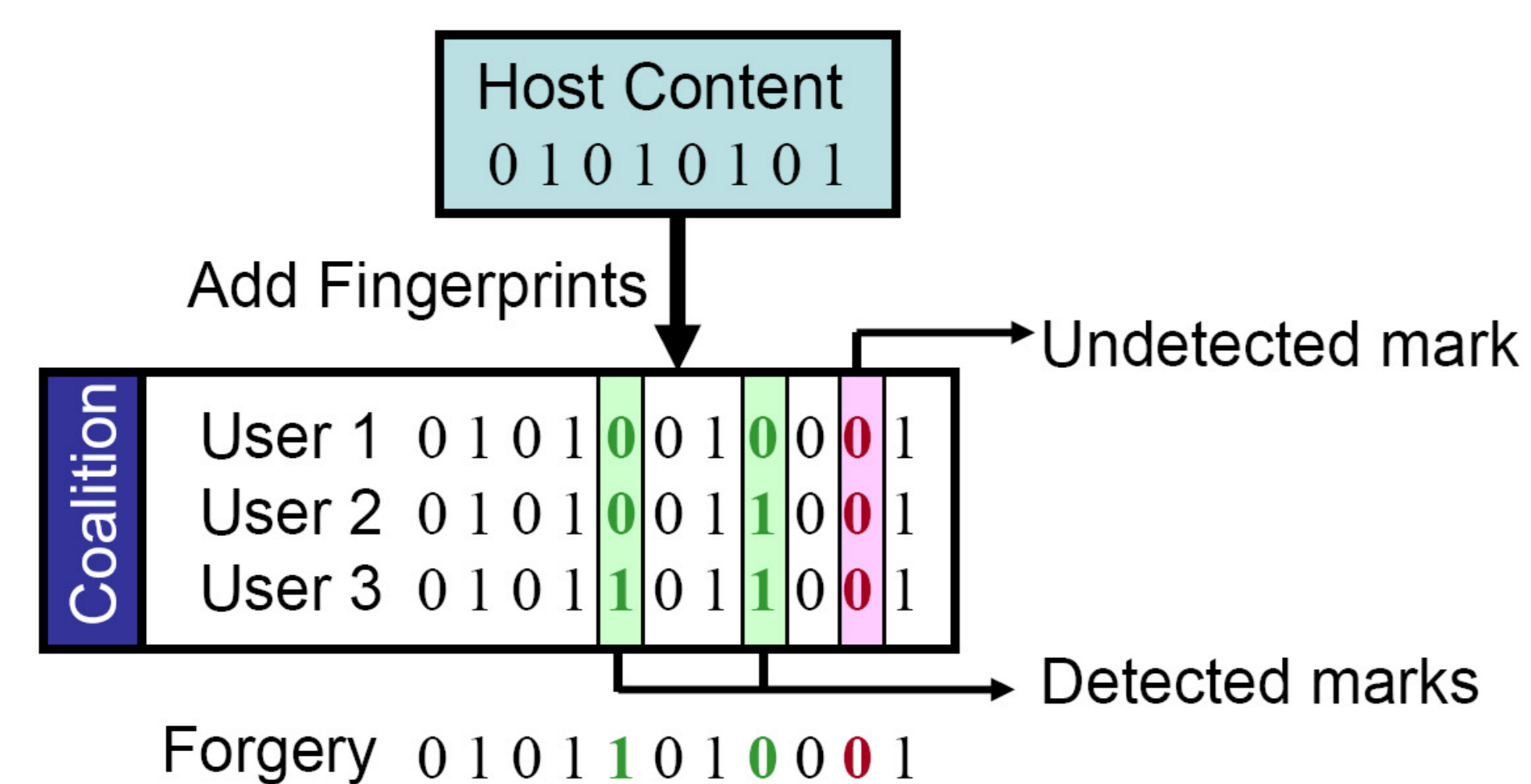
Fingerprinting is a technique for copyright protection. It was first proposed by Wagner in 1983 and has drawn a lot of attention in recent years. The content distributor embeds a unique mark, or *fingerprint*, within each licensed copy. By forming a group of users (*pirates*), the *coalition* can detect the fingerprints by inspecting the marks in each copy, and create a *forgery* that has only weak traces of their copies. A collusion-resistant fingerprinting system is designed to combat the collusive attacks.



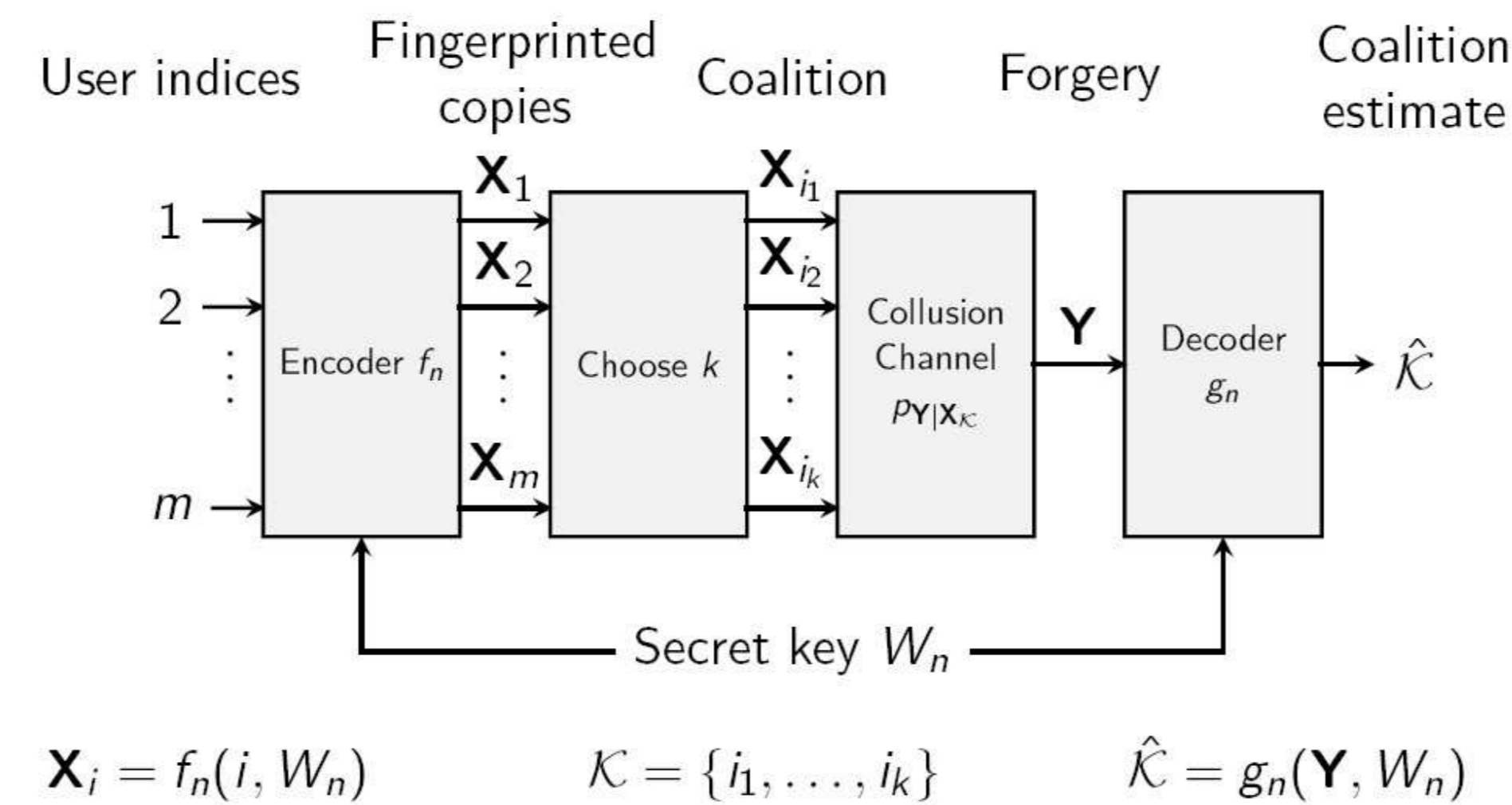
Using fingerprinting for tracing users (figure from Liu *et al.*, 2005)

### Marking Assumption

- First proposed by Boneh and Shaw in 1998
- The fingerprint is a set of redundant marks allocated throughout the host content
  - Locations of the marks are unknown to the pirates
- The coalitions may modify only those positions where they find a difference in their fingerprinted copies
- We only need to consider the fingerprint sequence in our analysis



## System Model



$$\mathbf{x}_i = f_n(i, W_n) \quad \mathcal{K} = \{i_1, \dots, i_k\} \quad \hat{\mathcal{K}} = g_n(\mathbf{Y}, W_n)$$

## Fingerprinting Capacity

Capacity is the fundamental measure of the ability to resist colluders of a scheme

### Collusion Channel

- Memoryless collusion channel

$$p_{\mathbf{Y}|\mathbf{X}_{\mathcal{K}}}(\mathbf{y}|\mathbf{x}_{\mathcal{K}}) = \prod_{j=1}^n p_{Y_j|X_{\mathcal{K},j}}(y_j|x_{\mathcal{K},j})$$

- Fairness property:  $p_{Y|X_{\mathcal{K}}} = p_{Y|X_{\pi\mathcal{K}}}$
- $p_{Y|X_{\mathcal{K}}}$  takes the form  $p_{Y|Z}$ 
  - $Z \triangleq \sum_{i \in \mathcal{K}} X_i \in \{0, 1, \dots, k\}$
- Let  $\mathbf{p} = (p_0, \dots, p_k)'$ , where  $p_z \triangleq p_{Y|Z}(1|z)$ ,  $z = 0, \dots, k$
- The marking assumption enforces that  $p_0 = 0$  and  $p_k = 1$

### Error Probabilities and Capacity

- Error events
  - $\hat{\mathcal{K}} \not\subseteq \mathcal{K}$ : Someone innocent falsely accused
  - $\mathcal{K} \cap \hat{\mathcal{K}} = \emptyset$ : No pirate caught
- Worst-case error probability:

$$P_e^*(F_n, G_n, k) = \max_{\substack{\mathcal{K} \subseteq \mathcal{M} \\ |\mathcal{K}| \leq k}} \max_{\mathbf{p}} \Pr \left[ (\hat{\mathcal{K}} \not\subseteq \mathcal{K}) \vee (\mathcal{K} \cap \hat{\mathcal{K}} = \emptyset) \right]$$

**Definition** (Moulin, 2008). A rate  $R$  is achievable for size- $k$  coalitions if there exists a sequence of fingerprinting codes  $(F_n, G_n)$  for  $m = \lceil 2^{nR} \rceil$  users such that

$$\lim_{n \rightarrow \infty} P_e^*(F_n, G_n, k) = 0.$$

Fingerprinting capacity  $C_k$  is the supremum of all achievable rates.

## Randomized Fingerprinting Code

### Encoder

- An  $(n, m)$  fingerprinting code  $\mathcal{C}$  is a set of  $m$  length- $n$  binary random sequences  $\mathbf{X}_1, \dots, \mathbf{X}_m$
- $W_j \sim p_W$  i.i.d.
  - $p_W$  can either be a continuous pdf or a discrete pmf
- $X_{i,j} \sim \text{Bernoulli}(W_j)$  i.i.d.

	$W_1$	$W_2$	$\dots$	$W_j$	$\dots$	$W_n$
User 1	$X_{1,1}$	$X_{1,2}$	$\dots$	$X_{1,j}$	$\dots$	$X_{1,n}$
User 2	$X_{2,1}$	$X_{2,2}$	$\dots$	$X_{2,j}$	$\dots$	$X_{2,n}$
$\vdots$	$\vdots$	$\vdots$	$\dots$	$\vdots$	$\dots$	$\vdots$
User $m$	$X_{m,1}$	$X_{m,2}$	$\dots$	$X_{m,j}$	$\dots$	$X_{m,n}$

### Decoder

- Joint decoder (capacity-achieving)

$$\hat{\mathcal{K}} = \operatorname{argmax}_{0 \leq |\mathcal{A}| \leq k} [I(\mathbf{x}_{\mathcal{A}}; \mathbf{y}|\mathbf{w}) - |\mathcal{A}|(R + \Delta)]$$

- Simple decoder (suboptimal)

$$\hat{\mathcal{K}} = \operatorname{argmax}_{1 \leq i \leq m} I(\mathbf{x}_i; \mathbf{y}|\mathbf{w})$$

## Mutual Information Games

**Theorem.**

$$C_k^{\text{joint}} \triangleq \max_{p_W} \min_{\mathbf{p}} \frac{1}{k} I(Z; Y|W) = \min_{\mathbf{p}} \max_w \frac{1}{k} I(Z; Y|W = w) = C_k$$

**Theorem.**

$$C_k^{\text{simple}} \triangleq \max_{p_W} \min_{\mathbf{p}} I(X_1; Y|W) = \min_{\mathbf{p}} \max_w I(X_1; Y|W = w) \leq C_k$$

## Secure Strategies and Capacity Bounds

- Tardos Embedding Distribution (Tardos, 2003)

$$p_W^\infty(w) = \frac{1}{\pi \sqrt{w(1-w)}}, w \in (0, 1)$$

- Interleaving Attack (Moulin, 2008)

$$p_z^\infty = \frac{z}{k}, \quad z = 0, \dots, k$$

## Upper Bounds

**Proposition.**

$$C_k^{\text{joint}} \leq \max_w \frac{1}{k} I_{\mathbf{p}^\infty}(Z; Y|W = w) \triangleq C_{k,U}^{\text{joint}} \leq \frac{1}{k^2 \ln 2}$$

**Proposition.**

$$C_k^{\text{simple}} \leq \max_w I_{\mathbf{p}^\infty}(X_1; Y|W = w) \triangleq C_{k,U}^{\text{simple}} = \frac{1}{k^2 \ln 2} + O\left(\frac{1}{k^4}\right)$$

## Lower Bounds

**Proposition.**

$$C_k^{\text{joint}} \geq \min_{\mathbf{p}} \frac{1}{k} I_{\mathbf{p}^\infty}(Z; Y|W) \triangleq C_{k,L}^{\text{joint}} \geq \frac{2}{k^2 \pi^2 \ln 2}$$

**Proposition.**

$$C_k^{\text{simple}} \geq \min_{\mathbf{p}} \frac{1}{k} I_{\mathbf{p}^\infty}(X_1; Y|W) \triangleq C_{k,L}^{\text{simple}} \geq \frac{2}{k^2 \pi^2 \ln 2}$$

## Numerical Results

