Deterministic Channel Design for Minimum Leakage

Arthur Américo, MHR. Khouzani, Pasquale Malacaria

School of Electronic Engineering and Computer Science
Queen Mary University of London

32nd IEEE CSF – 28 June 2019
Introduction
Introduction

- Systems often need to leak some sensitive information to function correctly/efficiently.
Introduction

- Systems often need to leak some sensitive information to function correctly/efficiently
  - A password checker always leaks information
Introduction

- Systems often need to leak some sensitive information to function correctly/efficiently
  - A password checker always leaks information
  - Eliminating all leakage from timing channels may lead to a substantial decrease in performance
Introduction

- Systems often need to leak some sensitive information to function correctly/efficiently
  - A password checker always leaks information
  - Eliminating all leakage from timing channels may lead to a substantial decrease in performance
- **Problem:** Find the system that minimizes information leakage while retaining functionality
Introduction

- Systems often need to leak some sensitive information to function correctly/efficiently
  - A password checker always leaks information
  - Eliminating all leakage from timing channels may lead to a substantial decrease in performance

- **Problem:** Find the system that minimizes information leakage while retaining functionality

- A general framework for this task was proposed in the CSF 2017 paper *Leakage Minimal Design: Universality, Limitations, and Applications*, by MHR. Khouzani and P. Malacaria
Introduction

► Systems often need to leak some sensitive information to function correctly/efficiently
  ► A password checker always leaks information
  ► Eliminating all leakage from timing channels may lead to a substantial decrease in performance

► Problem: Find the system that minimizes information leakage while retaining functionality

► A general framework for this task was proposed in the CSF 2017 paper *Leakage Minimal Design: Universality, Limitations, and Applications*, by MHR. Khouzani and P. Malacaria

Objective of this work

Study the application of this framework to deterministic systems
Preliminaries
A secret value is taken from a set $\mathcal{X} = \{x_1, \ldots, x_n\}$ according to a distribution $\pi$. An adversary, observing the behaviour of the system, may obtain some information about the secret value.
Quantitative Information Flow

- A secret value is taken from a set $\mathcal{X} = \{x_1, \ldots, x_n\}$ according to a distribution $\pi$.

- A system takes the secret value as input and produces an observable behaviour (or simply observable) in $\mathcal{Y} = \{y_1, \ldots, y_m\}$.
Quantitative Information Flow

- A secret value is taken from a set $\mathcal{X} = \{x_1, \ldots, x_n\}$ according to a distribution $\pi$
- A system takes the secret value as input and produces an observable behaviour (or simply observable) in $\mathcal{Y} = \{y_1, \ldots, y_m\}$
- An adversary, observing the behaviour of the system, may obtain some information about the secret value
Systems as Channels

- A system with inputs in $\mathcal{X}$ and observables in $\mathcal{Y}$ is modelled by a channel $C: \mathcal{X} \rightarrow \mathcal{Y}$. 

\[
\begin{array}{cccc}
C(y_1, y_2, y_3, y_4) & x_1 & 1/2 & 1/4 & 1/8 & 1/8 \\
x_2 & 1/4 & 1/2 & 1/4 & 0 \\
x_3 & 1 & 0 & 0 & 0 \\
\end{array}
\]
Systems as Channels

- A system with inputs in $\mathcal{X}$ and observables in $\mathcal{Y}$ is modelled by a channel $C : \mathcal{X} \rightarrow \mathcal{Y}$.
- $C(x, y)$ is the conditional probability that $y \in \mathcal{Y}$ will be produced given that the secret value is $x \in \mathcal{X}$.
Systems as Channels

- A system with inputs in $\mathcal{X}$ and observables in $\mathcal{Y}$ is modelled by a channel $C : \mathcal{X} \rightarrow \mathcal{Y}$.
- $C(x, y)$ is the conditional probability that $y \in \mathcal{Y}$ will be produced given that the secret value is $x \in \mathcal{X}$
  - $C(x, y) > 0 \quad \sum_y C(x, y) = 1$

<table>
<thead>
<tr>
<th></th>
<th>$y_1$</th>
<th>$y_2$</th>
<th>$y_3$</th>
<th>$y_4$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$x_1$</td>
<td>1/2</td>
<td>1/4</td>
<td>1/8</td>
<td>1/8</td>
</tr>
<tr>
<td>$x_2$</td>
<td>1/4</td>
<td>1/2</td>
<td>1/4</td>
<td>0</td>
</tr>
<tr>
<td>$x_3$</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>
Systems as Channels

▶ A system with inputs in $\mathcal{X}$ and observables in $\mathcal{Y}$ is modelled by a channel $C : \mathcal{X} \to \mathcal{Y}$.

▶ $C(x, y)$ is the conditional probability that $y \in \mathcal{Y}$ will be produced given that the secret value is $x \in \mathcal{X}$

  ▶ $C(x, y) > 0$  $\sum_y C(x, y) = 1$

<table>
<thead>
<tr>
<th>$C$</th>
<th>$y_1$</th>
<th>$y_2$</th>
<th>$y_3$</th>
<th>$y_4$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$x_1$</td>
<td>$1/2$</td>
<td>$1/4$</td>
<td>$1/8$</td>
<td>$1/8$</td>
</tr>
<tr>
<td>$x_2$</td>
<td>$1/4$</td>
<td>$1/2$</td>
<td>$1/4$</td>
<td>$0$</td>
</tr>
<tr>
<td>$x_3$</td>
<td>$1$</td>
<td>$0$</td>
<td>$0$</td>
<td>$0$</td>
</tr>
</tbody>
</table>

▶ In this work we focus on deterministic channels: $C(x, y) \in \{0, 1\}$
Systems as Channels

- A system with inputs in $\mathcal{X}$ and observables in $\mathcal{Y}$ is modelled by a channel $C : \mathcal{X} \rightarrow \mathcal{Y}$.

- $C(x, y)$ is the conditional probability that $y \in \mathcal{Y}$ will be produced given that the secret value is $x \in \mathcal{X}$.
  - $C(x, y) > 0$  \quad \sum_{y} C(x, y) = 1$

<table>
<thead>
<tr>
<th>$C$</th>
<th>$y_1$</th>
<th>$y_2$</th>
<th>$y_3$</th>
<th>$y_4$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$x_1$</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>$x_2$</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>$x_3$</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

- In this work we focus on deterministic channels: $C(x, y) \in \{0, 1\}$
How is information leaked?

- The adversary knows $\pi$ and $C$

<table>
<thead>
<tr>
<th>$\pi$</th>
<th>$C$</th>
</tr>
</thead>
<tbody>
<tr>
<td>1/3</td>
<td>$y_1$</td>
</tr>
<tr>
<td>1/4</td>
<td>$y_2$</td>
</tr>
<tr>
<td>1/4</td>
<td>$x_1$</td>
</tr>
<tr>
<td>1/4</td>
<td>$x_2$</td>
</tr>
<tr>
<td>1/6</td>
<td>$x_3$</td>
</tr>
</tbody>
</table>

- By observing $y$, the adversary updates the distribution from $\pi$ to $p_{X|y}$.
How is information leaked?

- The adversary knows $\pi$ and $C$
- Joint distribution $p(x, y) = \pi(x)C(x, y)$

<table>
<thead>
<tr>
<th>$p$</th>
<th>$y_1$</th>
<th>$y_2$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$x_1$</td>
<td>$1/3$</td>
<td>$0$</td>
</tr>
<tr>
<td>$x_2$</td>
<td>$0$</td>
<td>$1/4$</td>
</tr>
<tr>
<td>$x_3$</td>
<td>$0$</td>
<td>$1/4$</td>
</tr>
<tr>
<td>$x_4$</td>
<td>$1/6$</td>
<td>$0$</td>
</tr>
</tbody>
</table>

$p(y_1) = 1/2$

$p(y_2) = 1/2$
How is information leaked?

- The adversary knows $\pi$ and $C$
- Joint distribution $p(x, y) = \pi(x)C(x, y)$
- Marginal distribution $p(y) = \sum_{x \in X} p(x, y)$

<table>
<thead>
<tr>
<th>$p$</th>
<th>$y_1$</th>
<th>$y_2$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$x_1$</td>
<td>1/3</td>
<td>0</td>
</tr>
<tr>
<td>$x_2$</td>
<td>0</td>
<td>1/4</td>
</tr>
<tr>
<td>$x_3$</td>
<td>0</td>
<td>1/4</td>
</tr>
<tr>
<td>$x_4$</td>
<td>1/6</td>
<td>0</td>
</tr>
</tbody>
</table>

$p(y_1) = 1/2$

$p(y_2) = 1/2$
How is information leaked?

- The adversary knows \( \pi \) and \( C \)
- Joint distribution \( p(x, y) = \pi(x)C(x, y) \)
- Marginal distribution \( p(y) = \sum_{x \in X} p(x, y) \)
- Posterior distributions \( p_{X|y}(x) = \frac{p(x, y)}{p(y)} \)

| \( x \)  | \( p_{X|y_1} \) | \( p_{X|y_2} \) |
|--------|----------------|----------------|
| \( x_1 \) | \( \frac{2}{3} \) | 0 |
| \( x_2 \) | 0 | \( \frac{1}{2} \) |
| \( x_3 \) | 0 | \( \frac{1}{2} \) |
| \( x_4 \) | \( \frac{1}{3} \) | 0 |

\( p(y_1) = \frac{1}{2} \)
\( p(y_2) = \frac{1}{2} \)
How is information leaked?

- The adversary knows $\pi$ and $C$
- Joint distribution $p(x, y) = \pi(x)C(x, y)$
- Marginal distribution $p(y) = \sum_{x \in X} p(x, y)$
- Posterior distributions $p_{X|y}(x) = \frac{p(x,y)}{p(y)}$

| $x_i$ | $p_{X|y_1}$ | $p_{X|y_2}$ |
|-------|-------------|-------------|
| $x_1$ | $\frac{2}{3}$ | $0$         |
| $x_2$ | $0$         | $\frac{1}{2}$ |
| $x_3$ | $0$         | $\frac{1}{2}$ |
| $x_4$ | $\frac{1}{3}$ | $0$         |

$p(y_1) = \frac{1}{2}$

$p(y_2) = \frac{1}{2}$

- By observing $y$, the adversary updates the distribution from $\pi$ to $p_{X|y}$
Quantifying Information Leakage

- An entropy measure $H$ reflects how uncertain an adversary is about the secret value.

$H(\pi)$ = initial uncertainty

$H(\pi,C)$ = uncertainty after execution

Leakage = $H(\pi) - H(\pi,C)$
Quantifying Information Leakage

- An entropy measure $H$ reflects how uncertain an adversary is about the secret value.
- Many Choices: Shannon Entropy ($H_1$), min-entropy ($H_\infty$), guessing entropy ($H_G$) …
Quantifying Information Leakage

- An entropy measure $H$ reflects how uncertain an adversary is about the secret value.
- Many Choices: Shannon Entropy ($H_1$), min-entropy ($H_\infty$), guessing entropy ($H_G$) . . .
- $H(\pi) =$ initial uncertainty
Quantifying Information Leakage

- An entropy measure $H$ reflects how uncertain an adversary is about the secret value.
- Many Choices: Shannon Entropy ($H_1$), min-entropy ($H_\infty$), guessing entropy ($H_G$) . . .
- $H(\pi) =$ initial uncertainty
- $H(\pi, C) =$ uncertainty after execution
Quantifying Information Leakage

- An entropy measure $H$ reflects how uncertain an adversary is about the secret value.
- Many Choices: Shannon Entropy ($H_1$), min-entropy ($H_\infty$), guessing entropy ($H_G$)...
- $H(\pi) =$ initial uncertainty
- $H(\pi, C) =$ uncertainty after execution
- Leakage = $H(\pi) - H(\pi, C)$
Deterministic Channel Design

- Leakage $= H(\pi) - H(\pi, C)$
Deterministic Channel Design

- Leakage $= H(\pi) - H(\pi, C)$

### Deterministic Channel Design Problem

Given $\pi$ and a reasonable entropy measure $H$, find the deterministic channel $C$ that maximizes $H(\pi, C)$, respecting some operational constraints.
Deterministic Channel Design

- Leakage $= H(\pi) - H(\pi, C)$

**Deterministic Channel Design Problem**

Given $\pi$ and a reasonable entropy measure $H$, find the deterministic channel $C$ that maximizes $H(\pi, C)$, respecting some operational constraints

- Maximize $H(\pi, C) = \text{Minimize Leakage}$
Deterministic Channel Design

- Leakage = $H(\pi) - H(\pi, C)$

Deterministic Channel Design Problem

Given $\pi$ and a reasonable entropy measure $H$, find the deterministic channel $C$ that maximizes $H(\pi, C)$, respecting some operational constraints

- Maximize $H(\pi, C) = \text{Minimize Leakage}$
- What is a reasonable entropy?
Deterministic Channel Design

- Leakage $= H(\pi) - H(\pi, C)$

Deterministic Channel Design Problem

Given $\pi$ and a reasonable entropy measure $H$, find the deterministic channel $C$ that maximizes $H(\pi, C)$, respecting some operational constraints

- Maximize $H(\pi, C) = \text{Minimize Leakage}$
- What is a reasonable entropy?
- How should we model operational constraints?
What is a Reasonable Entropy?

- A entropy $H$ is **core-concave** if there is $\eta$, $F$ such that
  - $H(\pi) = \eta(F(\pi))$
  - $F$ is a real valued, continuous and concave function
  - $\eta : I \to \mathbb{R}$ is continuous and increasing
What is a Reasonable Entropy?

A entropy $H$ is core-concave if there is $\eta, F$ such that

$H(\pi) = \eta(F(\pi))$

$F$ is a real valued, continuous and concave function

$\eta : I \rightarrow \mathbb{R}$ is continuous and increasing

Prior entropy $H(\pi) = \eta(F(\pi))$
What is a Reasonable Entropy?

- A entropy $H$ is core-concave if there is $\eta$, $F$ such that
  - $H(\pi) = \eta(F(\pi))$
  - $F$ is a real valued, continuous and concave function
  - $\eta : I \to \mathbb{R}$ is continuous and increasing
- Prior entropy $H(\pi) = \eta(F(\pi))$
- Posterior entropy

$$H(\pi, C) = \eta \left( \sum_y p(y) F(p_{X|y}) \right)$$
What is a Reasonable Entropy?

- A entropy $H$ is **core-concave** if there is $\eta$, $F$ such that
  - $H(\pi) = \eta(F(\pi))$
  - $F$ is a real valued, continuous and concave function
  - $\eta : I \to \mathbb{R}$ is continuous and increasing
- Prior entropy $H(\pi) = \eta(F(\pi))$
- Posterior entropy
  
  $$H(\pi, C) = \eta \left( \sum_y p(y) F(p_x|y) \right)$$

- Generalizes most entropy measures in QIF
How Should We Model Operational Constraints?

- **Hard constraints**: A set $\Omega \subseteq \mathcal{X} \times \mathcal{Y}$ of which observables can be produced for each secret.
  - $C(x, y) > 0 \implies (x, y) \in \Omega$
How Should We Model Operational Constraints?

- **Hard constraints**: A set \( \Omega \subset \mathcal{X} \times \mathcal{Y} \) of which observables can be produced for each secret.

  - \( C(x, y) > 0 \implies (x, y) \in \Omega \)

\[
\Omega = \{(x_1, y_1), (x_1, y_2), (x_2, y_1), (x_2, y_3), (x_3, y_3)\}
\]
How Should We Model Operational Constraints?

- **Hard constraints**: A set $\Omega \subset X \times Y$ of which observables can be produced for each secret.
  
  - $C(x, y) > 0 \implies (x, y) \in \Omega$

$$\Omega = \{(x_1, y_1), (x_1, y_2), (x_2, y_1), (x_2, y_3), (x_3, y_3)\}$$

<table>
<thead>
<tr>
<th>$C$</th>
<th>$y_1$</th>
<th>$y_2$</th>
<th>$y_3$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$x_1$</td>
<td>?</td>
<td>?</td>
<td>0</td>
</tr>
<tr>
<td>$x_2$</td>
<td>?</td>
<td>0</td>
<td>?</td>
</tr>
<tr>
<td>$x_3$</td>
<td>0</td>
<td>0</td>
<td>?</td>
</tr>
</tbody>
</table>
How Should We Model Operational Constraints?

- **Hard constraints**: A set $\Omega \subset \mathcal{X} \times \mathcal{Y}$ of which observables can be produced for each secret.
  
  - $C(x, y) > 0 \implies (x, y) \in \Omega$

\[\Omega = \{(x_1, y_1), (x_1, y_2), (x_2, y_1), (x_2, y_3), (x_3, y_3)\}\]

<table>
<thead>
<tr>
<th>$C$</th>
<th>$y_1$</th>
<th>$y_2$</th>
<th>$y_3$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$x_1$</td>
<td>1</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>$x_2$</td>
<td>1</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>$x_3$</td>
<td>0</td>
<td>0</td>
<td>1</td>
</tr>
</tbody>
</table>
How Should We Model Operational Constraints?

- **Hard constraints**: A set $\Omega \subset \mathcal{X} \times \mathcal{Y}$ of which observables can be produced for each secret.
  - $C(x, y) > 0 \implies (x, y) \in \Omega$

$$
\Omega = \{ (x_1, y_1), (x_1, y_2), (x_2, y_1), (x_2, y_3), (x_3, y_3) \}
$$

<table>
<thead>
<tr>
<th>$C$</th>
<th>$y_1$</th>
<th>$y_2$</th>
<th>$y_3$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$x_1$</td>
<td>0</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>$x_2$</td>
<td>0</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>$x_3$</td>
<td>0</td>
<td>0</td>
<td>1</td>
</tr>
</tbody>
</table>
How to model operational constraints?

- **Soft constraints**: A function $u : \mathcal{X} \times \mathcal{Y} \to \mathbb{R}$ gives the “utility” of each pair of secret and observable
How to model operational constraints?

- **Soft constraints**: A function $u : \mathcal{X} \times \mathcal{Y} \rightarrow \mathbb{R}$ gives the “utility” of each pair of secret and observable
  - Execution time, difference between real and reported data, …
How to model operational constraints?

- **Soft constraints**: A function $u : \mathcal{X} \times \mathcal{Y} \to \mathbb{R}$ gives the “utility” of each pair of secret and observable
  - Execution time, difference between real and reported data, …
- **Constraint**: $E[u] = \sum_{x,y} \pi(x)C(x, y)u(x, y) \geq u_{\min}$
The general framework for the Channel Design Problem

(Probabilistic) Channel Design Problem (Khouzani and Malacaria, CSF 2017)

Find channel \( C : \mathcal{X} \rightarrow \mathcal{Y} \) that maximizes \( H(\pi, C) \) subject to

- \( C(x, y) > 0 \implies (x, y) \in \Omega \)
- \( \mathbb{E}[u] \geq u_{min} \)

\[
\begin{align*}
(\text{Probabilistic) Channel Design Problem (Khouzani and Malacaria, CSF 2017)})
\end{align*}
\]
The general framework for the Channel Design Problem

(Probabilistic) Channel Design Problem (Khouzani and Malacaria, CSF 2017)

Find channel $C : \mathcal{X} \to \mathcal{Y}$ that maximizes $H(\pi, C)$ subject to

- $C(x, y) > 0 \implies (x, y) \in \Omega$
- $\mathbb{E}[u] \geq u_{min}$

- Solved by convex programming (Karush-Kuhn Tucker conditions)
The Deterministic Channel Design Problem
The Deterministic Channel Design Problem

<table>
<thead>
<tr>
<th>Deterministic Channel Design Problem:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Find channel $C : \mathcal{X} \to \mathcal{Y}$ that maximizes $H(\pi, C)$ subject to</td>
</tr>
<tr>
<td>▶ $C(x, y) \in {0, 1}$</td>
</tr>
<tr>
<td>▶ $C(x, y) &gt; 0 \implies (x, y) \in \Omega$</td>
</tr>
<tr>
<td>▶ $\mathbb{E}[u] \geq u_{min}$</td>
</tr>
</tbody>
</table>
The Deterministic Channel Design Problem is NP-Hard
NP-Hardness

Theorem

*The Deterministic Channel Design Problem is NP-Hard*

*Proof:* reduction from the *Set Covering Problem*
The Deterministic Channel Design Problem is NP-Hard

Proof: reduction from the Set Covering Problem
Let $\mathcal{U}$ be a finite set and $\mathcal{C} \subset 2^{\mathcal{U}}$ a collection of subsets of $\mathcal{U}$
The Deterministic Channel Design Problem is NP-Hard

Proof: reduction from the Set Covering Problem
Let $\mathcal{U}$ be a finite set and $\mathcal{C} \subseteq 2^\mathcal{U}$ a collection of subsets of $\mathcal{U}$

There is a subcollection of $\mathcal{C}$ of size $k > 0$ that covers $\mathcal{U}$
**The Deterministic Channel Design Problem is NP-Hard**

*Proof:* reduction from the *Set Covering Problem*

Let \( \mathcal{U} \) be a finite set and \( \mathcal{C} \subseteq 2^{\mathcal{U}} \) a collection of subsets of \( \mathcal{U} \)

There is a subcollection of \( \mathcal{C} \) of size \( k > 0 \) that covers \( \mathcal{U} \)
NP-Hardness

Theorem

The Deterministic Channel Design Problem is NP-Hard

Proof: reduction from the Set Covering Problem

Let $\mathcal{U}$ be a finite set and $\mathcal{C} \subset 2^\mathcal{U}$ a collection of subsets of $\mathcal{U}$

There is a subcollection of $\mathcal{C}$ of size $k > 0$ that covers $\mathcal{U}$

There is a channel $C : \mathcal{U} \to \mathcal{C}$, with $H_\infty(\pi_u, C) \geq - \log k/|\mathcal{U}|$
NP-Hardness

Theorem

*The Deterministic Channel Design Problem is NP-Hard*

**Proof:** reduction from the Set Covering Problem

Let $\mathcal{U}$ be a finite set and $\mathcal{C} \subset 2^\mathcal{U}$ a collection of subsets of $\mathcal{U}$

There is a subcollection of $\mathcal{C}$ of size $k > 0$ that covers $\mathcal{U}$

\[ \uparrow \]

There is a channel $C : \mathcal{U} \to \mathcal{C}$, with

\[ H_\infty(\pi_u, C) \geq -\log \frac{k}{|\mathcal{U}|} \]

($\pi_u$ is the uniform distribution, and $\Omega = \{(x, y) \mid x \in y\}$)
Universality of the Solution

- The choice of entropy measure depends on the adversary’s interests and probabilities.
Universality of the Solution

- The choice of entropy measure depends on the adversary’s interests and probabilities.
- This may be outside of the designer’s control...
Universality of the Solution

- The choice of entropy measure depends on the adversary’s interests and probabilities.
- This may be outside of the designer’s control...
- Thus, a desirable property is universality: there is $C$ that is a solution for all core-concave entropies.
Universality of the Solution

- The choice of entropy measure depends on the adversary’s interests and probabilities.
- This may be outside of the designer’s control...
- Thus, a desirable property is universality: there is $C$ that is a solution for all core-concave entropies

<table>
<thead>
<tr>
<th>Theorem</th>
</tr>
</thead>
</table>

*In general, the Deterministic Channel Design Problem does not satisfy universality*
# Universality of the Solution

<table>
<thead>
<tr>
<th>Theorem</th>
</tr>
</thead>
<tbody>
<tr>
<td><em>In general, the Deterministic Channel Design Problem does not satisfy universality</em></td>
</tr>
</tbody>
</table>
Universality of the Solution

Theorem

*In general, the Deterministic Channel Design Problem does not satisfy universality*

**Proof** Let $\Omega = \{(x_1, y_1), (x_2, y_1), (x_1, y_2), (x_3, y_2), (x_2, y_3), (x_4, y_3)\}$

<table>
<thead>
<tr>
<th>$\pi$</th>
<th>$C$</th>
<th>$y_1$</th>
<th>$y_2$</th>
<th>$y_3$</th>
</tr>
</thead>
<tbody>
<tr>
<td>0.35</td>
<td>$x_1$</td>
<td>?</td>
<td>?</td>
<td>0</td>
</tr>
<tr>
<td>0.35</td>
<td>$x_2$</td>
<td>?</td>
<td>0</td>
<td>?</td>
</tr>
<tr>
<td>0.15</td>
<td>$x_3$</td>
<td>0</td>
<td>?</td>
<td>0</td>
</tr>
<tr>
<td>0.15</td>
<td>$x_4$</td>
<td>0</td>
<td>0</td>
<td>?</td>
</tr>
</tbody>
</table>
Universality of the Solution

Theorem

In general, the Deterministic Channel Design Problem does not satisfy universality

Proof Let $\Omega = \{(x_1, y_1), (x_2, y_1), (x_1, y_2), (x_3, y_2), (x_2, y_3), (x_4, y_3)\}$

<table>
<thead>
<tr>
<th>$\pi$</th>
<th>$C$</th>
<th>$y_1$</th>
<th>$y_2$</th>
<th>$y_3$</th>
</tr>
</thead>
<tbody>
<tr>
<td>0.35</td>
<td>$x_1$</td>
<td>1</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>0.35</td>
<td>$x_2$</td>
<td>1</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>0.15</td>
<td>$x_3$</td>
<td>0</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>0.15</td>
<td>$x_4$</td>
<td>0</td>
<td>0</td>
<td>1</td>
</tr>
</tbody>
</table>

Optimal for min-entropy
Universality of the Solution

**Theorem**

*In general, the Deterministic Channel Design Problem does not satisfy universality*

**Proof** Let \( \Omega = \{(x_1, y_1), (x_2, y_1), (x_1, y_2), (x_3, y_2), (x_2, y_3), (x_4, y_3)\} \)

\[
\begin{array}{c|ccc}
\pi & \pi_1 & \pi_2 & \pi_3 \\
0.35 & C & y_1 & y_2 & y_3 \\
0.35 & x_1 & 0 & 1 & 0 \\
0.35 & x_2 & 0 & 0 & 1 \\
0.15 & x_3 & 0 & 1 & 0 \\
0.15 & x_4 & 0 & 0 & 1 \\
\end{array}
\]

Optimal for Shannon entropy
The complete $k$-hypergraph problem
The Complete $k$-hypergraph Problem:

- The Complete $k$-hypergraph Problem: at most $k$ secret values can be mapped to each observable.

  $\mathcal{Y} = \{ A \subset X \mid |A| \leq k \}, \quad \Omega = \{ (x, y) \mid x \in y \}.$
The Complete $k$-hypergraph Problem:

- The Complete $k$-hypergraph Problem: at most $k$ secret values can be mapped to each observable
  - $\mathcal{Y} = \{ \mathcal{A} \subset \mathcal{X} \mid |\mathcal{A}| \leq k \}$, $\Omega = \{(x, y) \mid x \in y\}$.

- **Result:** There is a greedy solution to a subset of core-concave entropies, called leakage-supermodular
  - Includes most entropies used in QIF: Shannon entropy, min-entropy, guessing entropy...
Leakage-Supermodularity: Supermodular Functions

- **Lattice on** $\mathbb{R}^n_{\geq 0}$: Let $\mathbf{r} = (r_1, \ldots, r_n), \mathbf{s} = (s_1, \ldots, s_n) \in \mathbb{R}^n_{\geq 0}$
  - Join: $\mathbf{r} \vee \mathbf{s} = (\max(r_1, s_1), \ldots, \max(r_n, s_n))$
  - Meet: $\mathbf{r} \wedge \mathbf{s} = (\min(r_1, s_1), \ldots, \min(r_n, s_n))$
Leakage-Supermodularity: Supermodular Functions

- **Lattice on** $\mathbb{R}^n_{\geq 0}$: Let $\mathbf{r} = (r_1, \ldots, r_n), \mathbf{s} = (s_1, \ldots, s_n) \in \mathbb{R}^n_{\geq 0}$
  - **Join**: $\mathbf{r} \lor \mathbf{s} = (\max(r_1, s_1), \ldots, \max(r_n, s_n))$
  - **Meet**: $\mathbf{r} \land \mathbf{s} = (\min(r_1, s_1), \ldots, \min(r_n, s_n))$

**Example ($n = 2$):**

$\mathbf{r} = (r_1, r_2)$
$\mathbf{s} = (s_1, s_2)$
Leakage-Supermodularity: Supermodular Functions

- **Lattice on** $\mathbb{R}^n_{\geq 0}$: Let $r = (r_1, \ldots, r_n), s = (s_1, \ldots, s_n) \in \mathbb{R}^n_{\geq 0}$
  - **Join**: $r \lor s = (\max(r_1, s_1), \ldots, \max(r_n, s_n))$
  - **Meet**: $r \land s = (\min(r_1, s_1), \ldots, \min(r_n, s_n))$

**Example ($n = 2$):**
- $r = (r_1, r_2)$
- $s = (s_1, s_2)$

![Diagram showing lattice operations]

Example (n = 2):
- $r = (r_1, r_2)$
- $s = (s_1, s_2)$
- $r \lor s$
- $r \land s$
Leakage-Supermodularity: Supermodular Functions

- Lattice on $\mathbb{R}^n_{\geq 0}$: Let $r = (r_1, \ldots, r_n), s = (s_1, \ldots, s_n) \in \mathbb{R}^n_{\geq 0}$
  - Join: $r \lor s = (\max(r_1, s_1), \ldots, \max(r_n, s_n))$
  - Meet: $r \land s = (\min(r_1, s_1), \ldots, \min(r_n, s_n))$
- A function $\phi: \mathbb{R}^n_{\geq 0} \rightarrow \mathbb{R}$ is Supermodular if
  $$\phi(r \lor s) + \phi(r \land s) \geq \phi(r) + \phi(s)$$

Example ($n = 2$):
- $r = (r_1, r_2)$
- $s = (s_1, s_2)$
Leakage-Supermodularity: Supermodular Functions

▶ Lattice on $\mathbb{R}^n_{\geq 0}$: Let $r = (r_1, \ldots, r_n), s = (s_1, \ldots, s_n) \in \mathbb{R}^n_{\geq 0}$
  
  ▶ Join: $r \lor s = (\max(r_1, s_1), \ldots, \max(r_n, s_n))$
  
  ▶ Meet: $r \land s = (\min(r_1, s_1), \ldots, \min(r_n, s_n))$

▶ A function $\phi : \mathbb{R}^n_{\geq 0} \to \mathbb{R}$ is Supermodular if

$$\phi(r \lor s) + \phi(r \land s) \geq \phi(r) + \phi(s)$$

Example ($n = 2$):

$r = (r_1, r_2)$
$s = (s_1, s_2)$

Graphical representation showing the join and meet operations, with the supermodularity condition illustrated on a 2D plane.
Lattice on $\mathbb{R}^n_{\geq 0}$: Let $r = (r_1, \ldots, r_n), s = (s_1, \ldots, s_n) \in \mathbb{R}^n_{\geq 0}$

- Join: $r \lor s = (\max(r_1, s_1), \ldots, \max(r_n, s_n))$
- Meet: $r \land s = (\min(r_1, s_1), \ldots, \min(r_n, s_n))$

A function $\phi : \mathbb{R}^n_{\geq 0} \to \mathbb{R}$ is Supermodular if

$$\phi(r \lor s) + \phi(r \land s) \geq \phi(r) + \phi(s)$$

Example ($n = 2$):
- $r = (r_1, r_2)$
- $s = (s_1, s_2)$
- $r \land s$
- $r \lor s$
Leakage-Supermodular Entropies

For now on, we restrict our attention to entropies that are

- **Symmetric:** \( H(\pi_1, \ldots, \pi_n) = H(\pi_{\phi(1)}, \ldots, \pi_{\phi(n)}) \) for all permutations \( \phi \)
- **Expansible:** \( H(\pi_1, \ldots, \pi_n, 0) = H(\pi_1, \ldots, \pi_n) \)

Theorem

Shannon entropy, min-entropy, guessing entropy and Arimoto-Rényi entropies are leakage-supermodular
For now on, we restrict our attention to entropies that are

- **Symmetric:** $H(\pi_1, \ldots, \pi_n) = H(\pi_{\phi(1)}, \ldots, \pi_{\phi(n)})$ for all permutations $\phi$

- **Expansible:** $H(\pi_1, \ldots, \pi_n, 0) = H(\pi_1, \ldots, \pi_n)$

Given a core-concave $H$ for some $\eta, F$, define $G_F : \mathbb{R}_{\geq 0}^n \to \mathbb{R}$

$$G_F(r_1, \ldots, r_n) = \left( \sum_i r_i \right) F \left( \frac{r_1}{\sum_i r_i}, \ldots, \frac{r_n}{\sum_i r_i} \right)$$

Theorem

Shannon entropy, min-entropy, guessing entropy and Arimoto-Rényi entropies are leakage-supermodular
Leakage-Supermodular Entropies

- For now on, we restrict our attention to entropies that are
  - Symmetric: $H(\pi_1, \ldots, \pi_n) = H(\pi_{\phi(1)}, \ldots, \pi_{\phi(n)})$ for all permutations $\phi$
  - Expansible: $H(\pi_1, \ldots, \pi_n, 0) = H(\pi_1, \ldots, \pi_n)$

- Given a core-concave $H$ for some $\eta, F$, define $G_F : \mathbb{R}^n_{\geq 0} \rightarrow \mathbb{R}$

\[
G_F(r_1, \ldots, r_n) = \left(\sum_i r_i\right) F\left(\frac{r_1}{\sum_i r_i}, \ldots, \frac{r_n}{\sum_i r_i}\right)
\]

- $H$ is leakage-supermodular if $G_F$ is supermodular
Leakage-Supermodular Entropies

For now on, we restrict our attention to entropies that are

- **Symmetric:** \( H(\pi_1, \ldots, \pi_n) = H(\pi_{\phi(1)}, \ldots, \pi_{\phi(n)}) \) for all permutations \( \phi \)
- **Expansible:** \( H(\pi_1, \ldots, \pi_n, 0) = H(\pi_1, \ldots, \pi_n) \)

Given a core-concave \( H \) for some \( \eta, F \), define \( G_F : \mathbb{R}^n_{\geq 0} \to \mathbb{R} \)

\[
G_F(r_1, \ldots, r_n) = \left( \sum_i r_i \right) F \left( \frac{r_1}{\sum_i r_i}, \ldots, \frac{r_n}{\sum_i r_i} \right)
\]

\( H \) is leakage-supermodular if \( G_F \) is supermodular

**Theorem**

*Shannon entropy, min-entropy, guessing entropy and Arimoto-Rényi entropies are leakage-supermodular*
Leakage-Supermodular Entropies

- Relation to leakage:

\[
H(\pi, C) = \eta \left( \sum_y G_F (p(x_1, y), \ldots, p(x_n, y)) \right)
\]
Leakage-Supermodular Entropies

Relation to leakage:

\[ H(\pi, C) = \eta \left( \sum_{y} G_F (p(x_1, y), \ldots, p(x_n, y)) \right) \]

<table>
<thead>
<tr>
<th>( \pi )</th>
<th>( x_1 )</th>
<th>( y_1 )</th>
<th>( y_2 )</th>
</tr>
</thead>
<tbody>
<tr>
<td>1/3</td>
<td>0</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>1/4</td>
<td>0</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>1/4</td>
<td>0</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>1/6</td>
<td>1</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>
Leakage-Supermodular Entropies

Relation to leakage:

\[ H(\pi, C) = \eta \left( \sum_y G_F (p(x_1, y), \ldots, p(x_n, y)) \right) \]

<table>
<thead>
<tr>
<th>( p )</th>
<th>( y_1 )</th>
<th>( y_2 )</th>
</tr>
</thead>
<tbody>
<tr>
<td>( x_1 )</td>
<td>( \frac{1}{3} )</td>
<td>0</td>
</tr>
<tr>
<td>( x_2 )</td>
<td>0</td>
<td>( \frac{1}{4} )</td>
</tr>
<tr>
<td>( x_3 )</td>
<td>0</td>
<td>( \frac{1}{4} )</td>
</tr>
<tr>
<td>( x_4 )</td>
<td>( \frac{1}{6} )</td>
<td>0</td>
</tr>
</tbody>
</table>
Leakage-Supermodular Entropies

Relation to leakage:

\[ H(\pi, C) = \eta \left( \sum_y G_F (p(x_1, y), \ldots, p(x_n, y)) \right) \]

<table>
<thead>
<tr>
<th>( p )</th>
<th>( y_1 )</th>
<th>( y_2 )</th>
</tr>
</thead>
<tbody>
<tr>
<td>( x_1 )</td>
<td>1/3</td>
<td>0</td>
</tr>
<tr>
<td>( x_2 )</td>
<td>0</td>
<td>1/4</td>
</tr>
<tr>
<td>( x_3 )</td>
<td>0</td>
<td>1/4</td>
</tr>
<tr>
<td>( x_4 )</td>
<td>1/6</td>
<td>0</td>
</tr>
</tbody>
</table>

\[ H(\pi, C) = \eta \left( G_F(1/3, 0, 0, 1/6) + G_F(0, 1/4, 1/4, 0) \right) \]
A greedy solution

The $k$-hypergraph Problem

Let $\mathcal{Y} = \{ \mathcal{A} \subset \mathcal{X} \mid |\mathcal{A}| \leq k \}$. Find $C : \mathcal{X} \to \mathcal{Y}$ that maximizes $H(\pi, C)$, subject to $\Omega = \{(x, y) \in \mathcal{X} \times \mathcal{Y} \mid x \in y \}$
A greedy solution

The $k$-hypergraph Problem

Let $\mathcal{Y} = \{ A \subset \mathcal{X} \mid |A| \leq k \}$. Find $C : \mathcal{X} \to \mathcal{Y}$ that maximizes $H(\pi, C)$, subject to $\Omega = \{(x, y) \in \mathcal{X} \times \mathcal{Y} \mid x \in y\}$

- Order $\mathcal{X} = \{x_1, \ldots, x_n\}$ such that $\pi(x_1) \geq \cdots \geq \pi(x_n)$
A greedy solution

The $k$-hypergraph Problem

Let $\mathcal{Y} = \{\mathcal{A} \subset \mathcal{X} \mid |\mathcal{A}| \leq k\}$. Find $C : \mathcal{X} \rightarrow \mathcal{Y}$ that maximizes $H(\pi, C)$, subject to $\Omega = \{(x, y) \in \mathcal{X} \times \mathcal{Y} \mid x \in y\}$

- Order $\mathcal{X} = \{x_1, \ldots, x_n\}$ such that $\pi(x_1) \geq \cdots \geq \pi(x_n)$
- Build $C$ by mapping $x_1, \ldots, x_k$ to one output, $x_{k+1}, \ldots, x_{2k}$ to another and so on.
A greedy solution

The $k$-hypergraph Problem

Let $\mathcal{Y} = \{A \subset \mathcal{X} \mid |A| \leq k\}$. Find $C: \mathcal{X} \rightarrow \mathcal{Y}$ that maximizes $H(\pi, C)$, subject to $\Omega = \{(x, y) \in \mathcal{X} \times \mathcal{Y} \mid x \in y\}$

- Order $\mathcal{X} = \{x_1, \ldots, x_n\}$ such that $\pi(x_1) \geq \cdots \geq \pi(x_n)$
- Build $C$ by mapping $x_1, \ldots, x_k$ to one output, $x_{k+1}, \ldots, x_{2k}$ to another and so on.

Greedy solution for 8 secret values, and $k = 3$

| $\pi$  | $C$ | $y_1$ | $y_2$ | $y_3$ |
| 0.25  | $x_1$ | 1  | 0  | 0  |
| 0.20  | $x_2$ | 1  | 0  | 0  |
| 0.15  | $x_3$ | 1  | 0  | 0  |
| 0.13  | $x_4$ | 0  | 1  | 0  |
| 0.10  | $x_5$ | 0  | 1  | 0  |
| 0.08  | $x_6$ | 0  | 1  | 0  |
| 0.07  | $x_7$ | 0  | 0  | 1  |
| 0.02  | $x_8$ | 0  | 0  | 1  |
A greedy solution

Theorem

*For leakage-supermodular entropies, the greedy solution is optimal*
A greedy solution

**Theorem**

*For leakage-supermodular entropies, the greedy solution is optimal*

**Proof idea.**

<table>
<thead>
<tr>
<th>$\pi$</th>
<th>$C$</th>
<th>$y_1$</th>
<th>$y_2$</th>
<th>$y_3$</th>
</tr>
</thead>
<tbody>
<tr>
<td>0.3</td>
<td>$x_1$</td>
<td>1</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>0.3</td>
<td>$x_2$</td>
<td>0</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>0.2</td>
<td>$x_3$</td>
<td>1</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>0.1</td>
<td>$x_3$</td>
<td>0</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>0.1</td>
<td>$x_3$</td>
<td>0</td>
<td>0</td>
<td>1</td>
</tr>
</tbody>
</table>
A greedy solution

Theorem

For leakage-supermodular entropies, the greedy solution is optimal

Proof idea.

\[
\begin{array}{c|ccc}
  p & y_1 & y_2 & y_3 \\
  \hline
  x_1 & 0.3 & 0 & 0 \\
  x_2 & 0 & 0.3 & 0 \\
  x_3 & 0.2 & 0 & 0 \\
  x_3 & 0 & 0.1 & 0 \\
  x_3 & 0 & 0 & 0.1 \\
\end{array}
\]
A greedy solution

Theorem

For leakage-supermodular entropies, the greedy solution is optimal

Proof idea. $H(\pi, C) = \eta(G_F(0.3, 0.2) + G_F(0.3, 0.1) + G_F(0.1))$

<table>
<thead>
<tr>
<th>$p$</th>
<th>$y_1$</th>
<th>$y_2$</th>
<th>$y_3$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$x_1$</td>
<td>0.3</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>$x_2$</td>
<td>0</td>
<td>0.3</td>
<td>0</td>
</tr>
<tr>
<td>$x_3$</td>
<td>0.2</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>$x_3$</td>
<td>0</td>
<td>0.1</td>
<td>0</td>
</tr>
<tr>
<td>$x_3$</td>
<td>0</td>
<td>0</td>
<td>0.1</td>
</tr>
</tbody>
</table>
A greedy solution

Theorem

For leakage-supermodular entropies, the greedy solution is optimal

Proof idea. $H(\pi, C) = \eta(G_F(0.3, 0.2) + G_F(0.3, 0.1) + G_F(0.1))$

<table>
<thead>
<tr>
<th>$p$</th>
<th>$y_1$</th>
<th>$y_2$</th>
<th>$y_3$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$x_1$</td>
<td>0.3</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>$x_2$</td>
<td>0</td>
<td>0.3</td>
<td>0</td>
</tr>
<tr>
<td>$x_3$</td>
<td>0.2</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>$x_3$</td>
<td>0</td>
<td>0.1</td>
<td>0</td>
</tr>
<tr>
<td>$x_3$</td>
<td>0</td>
<td>0</td>
<td>0.1</td>
</tr>
</tbody>
</table>
## A greedy solution

### Theorem

*For leakage-supermodular entropies, the greedy solution is optimal*

### Proof idea

\[
H(\pi, C) = \eta(G_F(0.3, 0.2) + G_F(0.3, 0.1) + G_F(0.1))
\]

<table>
<thead>
<tr>
<th>(p')</th>
<th>(y_1)</th>
<th>(y_2)</th>
<th>(y_3)</th>
</tr>
</thead>
<tbody>
<tr>
<td>(x_1)</td>
<td>0.3</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>(x_2)</td>
<td>0.3</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>(x_3)</td>
<td>0</td>
<td>0.2</td>
<td>0</td>
</tr>
<tr>
<td>(x_3)</td>
<td>0</td>
<td>0.1</td>
<td>0</td>
</tr>
<tr>
<td>(x_3)</td>
<td>0</td>
<td>0</td>
<td>0.1</td>
</tr>
</tbody>
</table>
A greedy solution

**Theorem**

For leakage-supermodular entropies, the greedy solution is optimal

**Proof idea.** $H(\pi, C) = \eta(G_F(0.3, 0.2) + G_F(0.3, 0.1) + G_F(0.1))$

<table>
<thead>
<tr>
<th>$p'$</th>
<th>$y_1$</th>
<th>$y_2$</th>
<th>$y_3$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$x_1$</td>
<td>0.3</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>$x_2$</td>
<td>0.3</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>$x_3$</td>
<td>0</td>
<td>0.2</td>
<td>0</td>
</tr>
<tr>
<td>$x_3$</td>
<td>0</td>
<td>0.1</td>
<td>0</td>
</tr>
<tr>
<td>$x_3$</td>
<td>0</td>
<td>0</td>
<td>0.1</td>
</tr>
</tbody>
</table>
A greedy solution

Theorem

For leakage-supermodular entropies, the greedy solution is optimal

Proof idea. $H(\pi, C) = \eta(G_F(0.3, 0.2) + G_F(0.3, 0.1) + G_F(0.1))$

<table>
<thead>
<tr>
<th>$\pi$</th>
<th>$C'$</th>
<th>$y_1$</th>
<th>$y_2$</th>
<th>$y_3$</th>
</tr>
</thead>
<tbody>
<tr>
<td>0.3</td>
<td>$x_1$</td>
<td>1</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>0.3</td>
<td>$x_2$</td>
<td>1</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>0.2</td>
<td>$x_3$</td>
<td>0</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>0.1</td>
<td>$x_3$</td>
<td>0</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>0.1</td>
<td>$x_3$</td>
<td>0</td>
<td>0</td>
<td>1</td>
</tr>
</tbody>
</table>

$H(\pi, C') = \eta(G_F(0.3, 0.3) + G_F(0.2, 0.1) + G_F(0.1))$
A greedy solution

Thorem

For leakage-supermodular entropies, the greedy solution is optimal

Proof idea. $H(\pi, C) = \eta(G_F(0.3, 0.2) + G_F(0.3, 0.1) + G_F(0.1))$

<table>
<thead>
<tr>
<th>$\pi$</th>
<th>$C'$</th>
<th>$y_1$</th>
<th>$y_2$</th>
<th>$y_3$</th>
</tr>
</thead>
<tbody>
<tr>
<td>0.3</td>
<td>$x_1$</td>
<td>1</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>0.3</td>
<td>$x_2$</td>
<td>1</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>0.2</td>
<td>$x_3$</td>
<td>0</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>0.1</td>
<td>$x_3$</td>
<td>0</td>
<td>0</td>
<td>1</td>
</tr>
</tbody>
</table>

$H(\pi, C') = \eta(G_F(0.3, 0.3) + G_F(0.2, 0.1) + G_F(0.1))$

$(0.3, 0.3) = (0.3, 0.2) \lor (0.1, 0.3)$
A greedy solution

Theorem

For leakage-supermodular entropies, the greedy solution is optimal

Proof idea. $H(\pi, C') = \eta(G_F(0.3, 0.2) + G_F(0.3, 0.1) + G_F(0.1))$

<table>
<thead>
<tr>
<th>$\pi$</th>
<th>0.3</th>
<th>0.3</th>
<th>0.2</th>
<th>0.1</th>
<th>0.1</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>$x_1$</td>
<td>$x_2$</td>
<td>$x_3$</td>
<td>$x_3$</td>
<td>$x_3$</td>
</tr>
<tr>
<td>$y_1$</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>$y_2$</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>$y_3$</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

$H(\pi, C') = \eta(G_F(0.3, 0.3) + G_F(0.2, 0.1) + G_F(0.1))$

$(0.1, 0.2) = (0.3, 0.2) \land (0.1, 0.3)$
A greedy solution

Theorem

For leakage-supermodular entropies, the greedy solution is optimal

Proof idea. $H(\pi, C) = \eta(G_F(0.3, 0.2) + G_F(0.3, 0.1) + G_F(0.1))$

<table>
<thead>
<tr>
<th>$\pi$</th>
<th>$C'$</th>
<th>$y_1$</th>
<th>$y_2$</th>
<th>$y_3$</th>
</tr>
</thead>
<tbody>
<tr>
<td>0.3</td>
<td>$x_1$</td>
<td>1</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>0.3</td>
<td>$x_2$</td>
<td>1</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>0.2</td>
<td>$x_3$</td>
<td>0</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>0.1</td>
<td>$x_3$</td>
<td>0</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>0.1</td>
<td>$x_3$</td>
<td>0</td>
<td>0</td>
<td>1</td>
</tr>
</tbody>
</table>

$H(\pi, C') = \eta(G_F(0.3, 0.3) + G_F(0.2, 0.1) + G_F(0.1))$

$H(\pi, C') \geq H(\pi, C)$
Experimental comparison

Size of input set

Optimal, \((H_1)\)
Optimal \((H_{\infty})\)
Random \((H_1)\)
Random \((H_{\infty})\)
Un-optimal \((H_1)\)
Un-optimal \((H_{\infty})\)
Deterministic Channels as a Solution for Multiple Executions
Deterministic Channels as a Solution for Multiple Executions

Often, a system is executed multiple times for a fixed secret value
Deterministic Channels as a Solution for Multiple Executions

- Often, a system is executed multiple times for a fixed secret value
- How do we design an optimal system in this scenario?
Deterministic Channels as a Solution for Multiple Executions

<table>
<thead>
<tr>
<th>C</th>
<th>$y_1$</th>
<th>$y_2$</th>
<th>$y_3$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$x_1$</td>
<td>??</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>$x_2$</td>
<td>?</td>
<td>0</td>
<td>?</td>
</tr>
<tr>
<td>$x_3$</td>
<td>0</td>
<td>?</td>
<td>?</td>
</tr>
<tr>
<td>$x_4$</td>
<td>?</td>
<td>0</td>
<td>?</td>
</tr>
<tr>
<td>$x_5$</td>
<td>?</td>
<td>?</td>
<td>?</td>
</tr>
</tbody>
</table>
Deterministic Channels as a Solution for Multiple Executions

<table>
<thead>
<tr>
<th>C</th>
<th>$y_1$</th>
<th>$y_2$</th>
<th>$y_3$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$x_1$</td>
<td>$\frac{1}{2}$</td>
<td>$\frac{1}{2}$</td>
<td>0</td>
</tr>
<tr>
<td>$x_2$</td>
<td>$\frac{1}{3}$</td>
<td>0</td>
<td>$\frac{2}{3}$</td>
</tr>
<tr>
<td>$x_3$</td>
<td>0</td>
<td>$\frac{3}{4}$</td>
<td>$\frac{1}{4}$</td>
</tr>
<tr>
<td>$x_4$</td>
<td>$\frac{1}{3}$</td>
<td>0</td>
<td>$\frac{2}{3}$</td>
</tr>
<tr>
<td>$x_5$</td>
<td>$\frac{3}{5}$</td>
<td>$\frac{1}{5}$</td>
<td>$\frac{1}{5}$</td>
</tr>
</tbody>
</table>
Deterministic Channels as a Solution for Multiple Executions

<table>
<thead>
<tr>
<th>$C$</th>
<th>$y_1$</th>
<th>$y_2$</th>
<th>$y_3$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$x_1$</td>
<td>$\frac{1}{2}$</td>
<td>$\frac{1}{2}$</td>
<td>0</td>
</tr>
<tr>
<td>$x_2$</td>
<td>$\frac{1}{3}$</td>
<td>0</td>
<td>$\frac{2}{3}$</td>
</tr>
<tr>
<td>$x_3$</td>
<td>0</td>
<td>$\frac{3}{4}$</td>
<td>$\frac{1}{4}$</td>
</tr>
<tr>
<td>$x_4$</td>
<td>$\frac{1}{3}$</td>
<td>0</td>
<td>$\frac{2}{3}$</td>
</tr>
<tr>
<td>$x_5$</td>
<td>$\frac{3}{5}$</td>
<td>$\frac{1}{5}$</td>
<td>$\frac{1}{5}$</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>$C$</th>
<th>$[x_1]$</th>
<th>$[x_2]$</th>
<th>$[x_3]$</th>
<th>$[x_5]$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$x_1$</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>$x_2$</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>$x_3$</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>$x_4$</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>$x_5$</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
</tr>
</tbody>
</table>
Deterministic Channels as a Solution for Multiple Executions

<table>
<thead>
<tr>
<th>$C$</th>
<th>$y_1$</th>
<th>$y_2$</th>
<th>$y_3$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$x_1$</td>
<td>0</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>$x_2$</td>
<td>0</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>$x_3$</td>
<td>0</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>$x_4$</td>
<td>0</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>$x_5$</td>
<td>0</td>
<td>1</td>
<td>0</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>$C$</th>
<th>$[x_1]$</th>
<th>$[x_2]$</th>
<th>$[x_3]$</th>
<th>$[x_5]$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$x_1$</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>$x_2$</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>$x_3$</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>$x_4$</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>$x_5$</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
</tr>
</tbody>
</table>
Deterministic Channels as a Solution for Multiple Executions

**Proposition**

Let $C$ be a probabilistic channel respecting the operational constraints. Then, there is a deterministic channel $D$ that respects the same constraints and asymptotically leaks at most as much information as $C$. 
Deterministic Channels as a Solution for Multiple Executions

Proposition

Let $C$ be a probabilistic channel respecting the operational constraints. Then, there is a deterministic channel $D$ that respects the same constraints and asymptotically leaks at most as much information as $C$.

Thus, the deterministic solution to the design problem is asymptotically optimal.
Conclusions and Contributions
Conclusions and Contributions

In this work we...
Conclusions and Contributions

In this work we...

▶ Investigated the Deterministic Channel Design Problem: NP-hardness and non-universality

▶ Established a greedy solution for the $k$-hypergraph problem which is optimal for the most common entropy measures

▶ Introduced leakage-supermodularity, which may be a useful concept for future work in QIF

▶ Channel Ordering and Supermodularity – to appear at IEEE ITW 2019

▶ Proved that, if a system is to be executed multiple times, the deterministic solution is optimal when the number of executions is very large
Conclusions and Contributions

In this work we...

- Investigated the Deterministic Channel Design Problem: NP-hardness and non-universality
- Established a greedy solution for the $k$-hypergraph problem which is optimal for the most common entropy measures
- Introduced leakage-supermodularity, which may be a useful concept for future work in QIF
- Channel Ordering and Supermodularity – to appear at IEEE ITW 2019
- Proved that, if a system is to be executed multiple times, the deterministic solution is optimal when the number of executions is very large
Conclusions and Contributions

In this work we...

▶ Investigated the Deterministic Channel Design Problem: NP-hardness and non-universality
▶ Established a greedy solution for the $k$-hypergraph problem which is optimal for the most common entropy measures
▶ Introduced leakage-supermodularity, which may be a useful concept for future work in QIF
Conclusions and Contributions

In this work we...

▶ Investigated the Deterministic Channel Design Problem: NP-hardness and non-universality
▶ Established a greedy solution for the $k$-hypergraph problem which is optimal for the most common entropy measures
▶ Introduced leakage-supermodularity, which may be a useful concept for future work in QIF
  ▶ *Channel Ordering and Supermodularity* – to appear at IEEE ITW 2019
In this work we...

- Investigated the Deterministic Channel Design Problem: NP-hardness and non-universality
- Established a greedy solution for the $k$-hypergraph problem which is optimal for the most common entropy measures
- Introduced leakage-supermodularity, which may be a useful concept for future work in QIF
  - *Channel Ordering and Supermodularity* – to appear at IEEE ITW 2019
- Proved that, if a system is to be executed multiple times, the deterministic solution is optimal when the number of executions is very large