Formal Privacy Analyses for Open Banking

Luigi D. C. Soares[1,2], Mário S. Alvim[1], Di Bu[2], Natasha Fernandes[2] and Yin Liao[2]

6th December 2024

[1]UFMG (Brazil) [2]Macquarie University (Australia)

Open Banking — Pros

- Gives customers control over the sharing of their financial data

Open Banking — Pros

- Gives customers control over the sharing of their financial data
- Facilitates access to new financial products or services

Open Banking — Pros

- Gives customers control over the sharing of their financial data
- Facilitates access to new financial products or services
- Smaller fintechs can evaluate customers without requiring negotiation with other banks or relying on customer-provided information

Open Banking — Concerns

- It involves the sharing of sensitive microdata

Open Banking — Concerns

- It involves the sharing of sensitive microdata
- In principle, under Open Banking companies should request from customers only the kind of information that their product requires. But, descriptions

Open Banking — Concerns

- It involves the sharing of sensitive microdata
- In principle, under Open Banking companies should request from customers only the kind of information that their product requires. But, descriptions
    - Are mandatory and are used by companies in multiple ways

Open Banking — Concerns

- It involves the sharing of sensitive microdata
- In principle, under Open Banking companies should request from customers only the kind of information that their product requires. But, descriptions
  - Are mandatory and are used by companies in multiple ways
  - Carry way more information than what companies need

Open Banking — Concerns

- It involves the sharing of sensitive microdata
- In principle, under Open Banking companies should request from customers only the kind of information that their product requires. But, descriptions
    - Are mandatory and are used by companies in multiple ways
    - Carry way more information than what companies need
    - May contain a variety of sensitive information

Open Banking — Concerns

- It involves the sharing of sensitive microdata
- In principle, under Open Banking companies should request from customers only the kind of information that their product requires. But, descriptions
  - Are mandatory and are used by companies in multiple ways
  - Carry way more information than what companies need
  - May contain a variety of sensitive information
- Goal: Assess privacy risks involved when sharing financial data via Open Banking

Main Result — Transaction-History Recovery Risk

- Attacker gains access to data collected via Open Banking

Main Result — Transaction-History Recovery Risk

- Attacker gains access to data collected via Open Banking
- Attacker combines the dataset with external, auxiliary information

Main Result — Transaction-History Recovery Risk

- Attacker gains access to data collected via Open Banking
- Attacker combines the dataset with external, auxiliary information
- Attacker tries to re-identify the transaction history of a target

Main Result — Transaction-History Recovery Risk

- Attacker gains access to data collected via Open Banking
- Attacker combines the dataset with external, auxiliary information
- Attacker tries to re-identify the transaction history of a target

	Re-identification Risk			
Auxiliary Information	1 month	2 months	3 months	4 months
Date, Payee, Category				
Date, Amount				
Date, Payee, Amount				
Date, Amount, Category				
Date, Payee, Amount, Category				

Main Result — Transaction-History Recovery Risk

- Attacker gains access to data collected via Open Banking
- Attacker combines the dataset with external, auxiliary information
- Attacker tries to re-identify the transaction history of a target

	Re-identification Risk			
Auxiliary Information	1 month	2 months	3 months	4 months
Date, Payee, Category	5.30%			
Date, Amount	26.6%			
Date, Payee, Amount	52.1%			
Date, Amount, Category	43.7%			
Date, Payee, Amount, Category	54.4%			

Main Result — Transaction-History Recovery Risk

- Attacker gains access to data collected via Open Banking
- Attacker combines the dataset with external, auxiliary information
- Attacker tries to re-identify the transaction history of a target

	Re-identification Risk			
Auxiliary Information	1 month	2 months	3 months	4 months
Date, Payee, Category	5.30%	29.2%		
Date, Amount	26.6%	80.7%		
Date, Payee, Amount	52.1%	91.1%		
Date, Amount, Category	43.7%	91.7%		
Date, Payee, Amount, Category	54.4%	93.6%		

Main Result — Transaction-History Recovery Risk

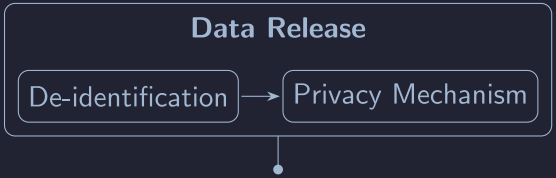
- Attacker gains access to data collected via Open Banking
- Attacker combines the dataset with external, auxiliary information
- Attacker tries to re-identify the transaction history of a target

	Re-identification Risk			
Auxiliary Information	1 month	2 months	3 months	4 months
Date, Payee, Category	5.30%	29.2%	60.9%	
Date, Amount	26.6%	80.7%	97.5%	
Date, Payee, Amount	52.1%	91.1%	99.2%	
Date, Amount, Category	43.7%	91.7%	99.4%	
Date, Payee, Amount, Category	54.4%	93.6%	99.6%	

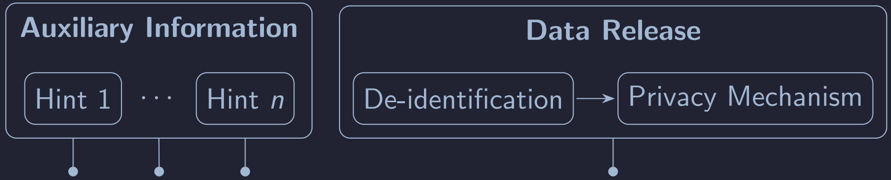
Main Result — Transaction-History Recovery Risk

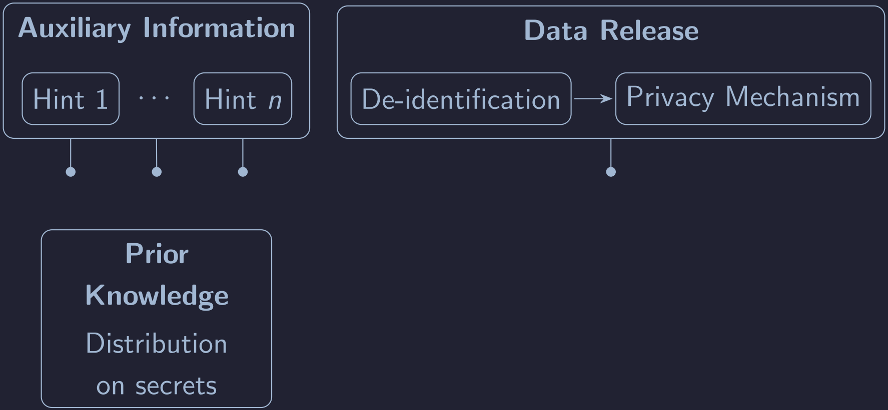
- Attacker gains access to data collected via Open Banking
- Attacker combines the dataset with external, auxiliary information
- Attacker tries to re-identify the transaction history of a target

	Re-identification Risk			
Auxiliary Information	1 month	2 months	3 months	4 months
Date, Payee, Category	5.30%	29.2%	60.9%	83.6%
Date, Amount	26.6%	80.7%	97.5%	99.8%
Date, Payee, Amount	52.1%	91.1%	99.2%	99.9%
Date, Amount, Category	43.7%	91.7%	99.4%	100%
Date, Payee, Amount, Category	54.4%	93.6%	99.6%	100%

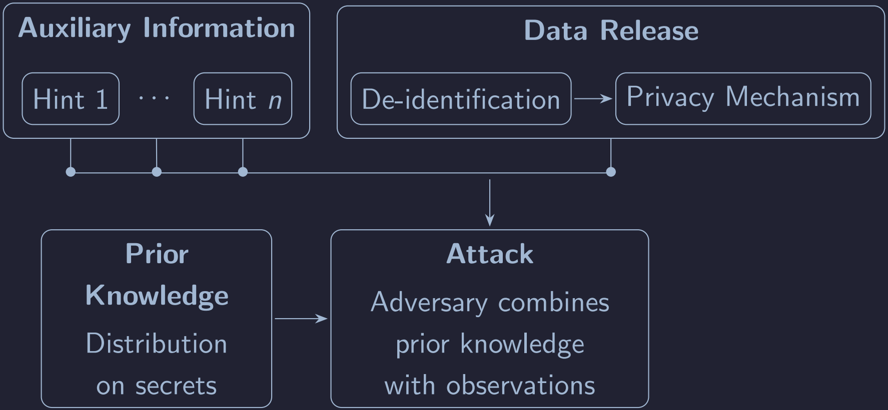

Data Release
De-identification
Privacy Mechanism

Formal Model — Attacks Against Data Releases

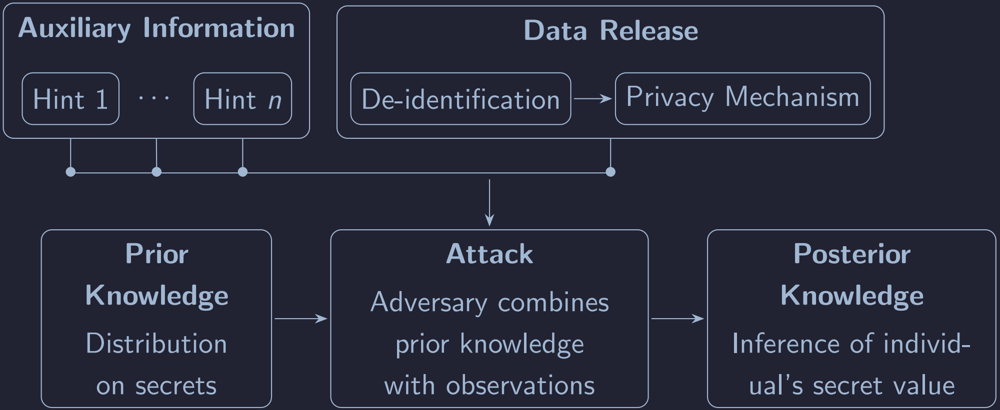



Auxiliary Information
Hint 1
· · ·
Hint n
Data Release
De-identification
Privacy Mechanism
Prior
Knowledge
Distribution
on secrets

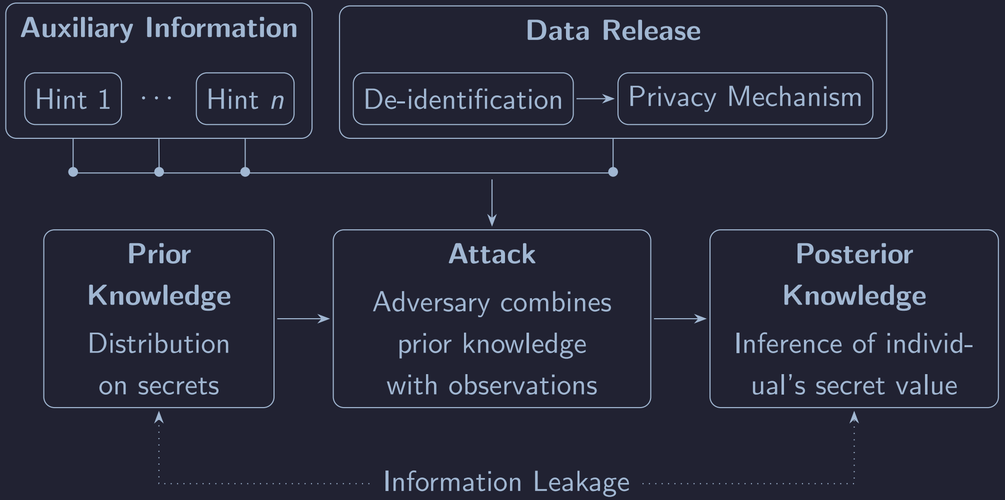
Formal Model — Attacks Against Data Releases

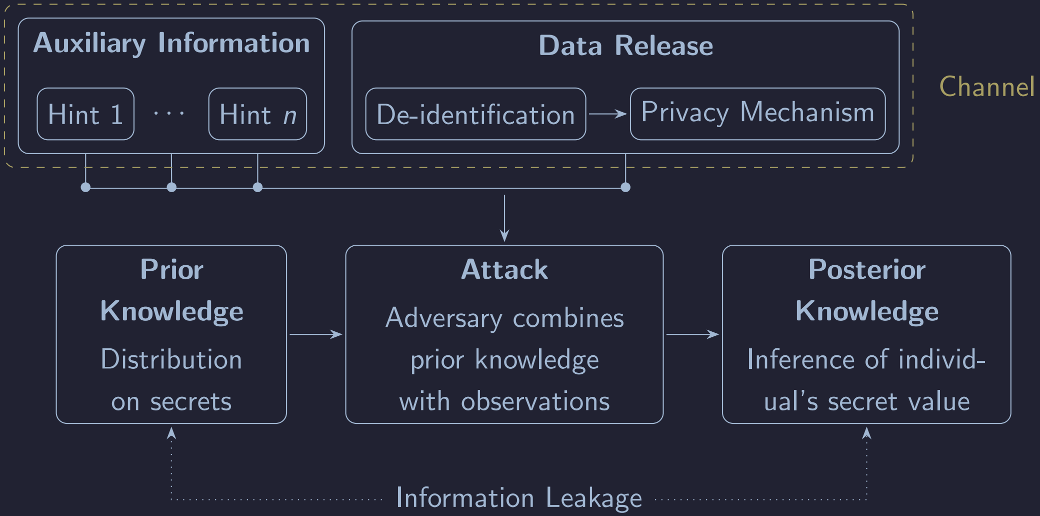


Formal Model — Attacks Against Data Releases



Formal Model — Attacks Against Data Releases




Auxiliary Information
Hint 1
···
Hint n
Data Release
De-identification
Privacy Mechanism
Channel
Prior
Knowledge
Distribution
on secrets
Attack
Adversary combines
prior knowledge
with observations
Posterior
Knowledge
Inference of individ-
ual's secret value
Information Leakage

- We use the mathematical framework of Quantitative Information Flow (QIF)

Formal Model — Modelling with Channels

- We use the mathematical framework of Quantitative Information Flow (QIF)
- Let $d = \langle 1\colon \vec{t}_1, 2\colon \vec{t}_2, 3\colon \vec{t}_3, 4\colon \vec{t}_4, 5\colon \vec{t}_5 \rangle$ be a de-identified dataset, where each $\vec{t}_i$ is the transaction history of customer with id i

Formal Model — **Modelling with Channels**

- We use the mathematical framework of Quantitative Information Flow (QIF)
- Let $d = \langle 1\colon \vec{t}_1, 2\colon \vec{t}_2, 3\colon \vec{t}_3, 4\colon \vec{t}_4, 5\colon \vec{t}_5 \rangle$ be a de-identified dataset, where each $\vec{t}_i$ is the transaction history of customer with id i

$$x_1 = \langle \text{Lineu}\colon \vec{t}_1, \text{Nenê}\colon \vec{t}_2, \text{Agostinho}\colon \vec{t}_3, \text{Tuco}\colon \vec{t}_4, \text{Bebel}\colon \vec{t}_5 \rangle \longrightarrow d$$

- We use the mathematical framework of Quantitative Information Flow (QIF)
- Let $d = \langle 1\colon \vec{t}_1, 2\colon \vec{t}_2, 3\colon \vec{t}_3, 4\colon \vec{t}_4, 5\colon \vec{t}_5 \rangle$ be a de-identified dataset, where each $\vec{t}_i$ is the transaction history of customer with id i

$$
\begin{tikzcd}
x_1 = \langle \text{Lineu: } \vec{t}_1, \text{Nenê: } \vec{t}_2, \text{Agostinho: } \vec{t}_3, \text{Tuco: } \vec{t}_4, \text{Bebel: } \vec{t}_5 \rangle \arrow[dr] & \\
x_2 = \langle \text{Lineu: } \vec{t}_2, \text{Nenê: } \vec{t}_3, \text{Agostinho: } \vec{t}_4, \text{Tuco: } \vec{t}_5, \text{Bebel: } \vec{t}_1 \rangle \arrow[r] & d
\end{tikzcd}
$$

- We use the mathematical framework of Quantitative Information Flow (QIF)
- Let $d = \langle 1\colon \vec{t}_1, 2\colon \vec{t}_2, 3\colon \vec{t}_3, 4\colon \vec{t}_4, 5\colon \vec{t}_5 \rangle$ be a de-identified dataset, where each $\vec{t}_i$ is the transaction history of customer with id i

$$
\begin{tikzcd}
x_1 = \langle \text{Lineu}\colon \vec{t}_1, \text{Nenê}\colon \vec{t}_2, \text{Agostinho}\colon \vec{t}_3, \text{Tuco}\colon \vec{t}_4, \text{Bebel}\colon \vec{t}_5 \rangle \arrow[dr] & \\
x_2 = \langle \text{Lineu}\colon \vec{t}_2, \text{Nenê}\colon \vec{t}_3, \text{Agostinho}\colon \vec{t}_4, \text{Tuco}\colon \vec{t}_5, \text{Bebel}\colon \vec{t}_1 \rangle \arrow[r] & d \\
x_3 = \langle \text{Lineu}\colon \vec{t}_3, \text{Nenê}\colon \vec{t}_4, \text{Agostinho}\colon \vec{t}_5, \text{Tuco}\colon \vec{t}_1, \text{Bebel}\colon \vec{t}_2 \rangle \arrow[ur] &
\end{tikzcd}
$$

Formal Model — Modelling with Channels

- We use the mathematical framework of Quantitative Information Flow (QIF)
- Let $d = \langle 1\colon \vec{t}_1, 2\colon \vec{t}_2, 3\colon \vec{t}_3, 4\colon \vec{t}_4, 5\colon \vec{t}_5 \rangle$ be a de-identified dataset, where each $\vec{t}_i$ is the transaction history of customer with id i

$$
\begin{tikzcd}
x_1 = \langle \text{Lineu}\colon \vec{t}_1, \text{Nenê}\colon \vec{t}_2, \text{Agostinho}\colon \vec{t}_3, \text{Tuco}\colon \vec{t}_4, \text{Bebel}\colon \vec{t}_5 \rangle \arrow[dr] & \\
x_2 = \langle \text{Lineu}\colon \vec{t}_2, \text{Nenê}\colon \vec{t}_3, \text{Agostinho}\colon \vec{t}_4, \text{Tuco}\colon \vec{t}_5, \text{Bebel}\colon \vec{t}_1 \rangle \arrow[r] & d \\
x_3 = \langle \text{Lineu}\colon \vec{t}_3, \text{Nenê}\colon \vec{t}_4, \text{Agostinho}\colon \vec{t}_5, \text{Tuco}\colon \vec{t}_1, \text{Bebel}\colon \vec{t}_2 \rangle \arrow[ur] &
\end{tikzcd}
$$

- In addition to observing a de-identified dataset d, an attacker might also know that their target, say Lineu, recurringly buys at a Pastry Shop and Araujo

- We use the mathematical framework of Quantitative Information Flow (QIF)
- Let $d = \langle 1\colon \vec{t}_1, 2\colon \vec{t}_2, 3\colon \vec{t}_3, 4\colon \vec{t}_4, 5\colon \vec{t}_5 \rangle$ be a de-identified dataset, where each $\vec{t}_i$ is the transaction history of customer with id i

$$\begin{array}{lcl}
x_1 = \langle \text{Lineu}\colon \vec{t}_1, \text{Nenê}\colon \vec{t}_2, \text{Agostinho}\colon \vec{t}_3, \text{Tuco}\colon \vec{t}_4, \text{Bebel}\colon \vec{t}_5 \rangle & \searrow & \\
x_2 = \langle \text{Lineu}\colon \vec{t}_2, \text{Nenê}\colon \vec{t}_3, \text{Agostinho}\colon \vec{t}_4, \text{Tuco}\colon \vec{t}_5, \text{Bebel}\colon \vec{t}_1 \rangle & \longrightarrow & d \\
x_3 = \langle \text{Lineu}\colon \vec{t}_3, \text{Nenê}\colon \vec{t}_4, \text{Agostinho}\colon \vec{t}_5, \text{Tuco}\colon \vec{t}_1, \text{Bebel}\colon \vec{t}_2 \rangle & \nearrow &
\end{array}$$

- In addition to observing a de-identified dataset d, an attacker might also know that their target, say Lineu, recurringly buys at a Pastry Shop and Araujo
- With 2 months of data, the attacker could observe, e.g., $\langle \text{Pastry Shop}, \text{Araujo}, d \rangle$

$$
\begin{array}{c|cccc}
C^{\text{Lineu}} & \langle \text{Pastry}, \text{Araujo}, d\rangle & \langle \text{Clinic}, \text{Araujo}, d\rangle & \langle \text{Clinic}, \text{Pastry}, d\rangle & \cdots \\
\hline
\begin{array}{c} x_1 \\ x_2 \\ x_3 \\ x_4 \\ x_5 \\ \vdots \end{array} &
\multicolumn{4}{l}{\left[\begin{array}{cccc}
\frac{1}{2} & \frac{1}{2} & 0 & \cdots \\
0 & 0 & 0 & \cdots \\
0 & \frac{1}{6} & \frac{1}{6} & \cdots \\
0 & 0 & 0 & \cdots \\
0 & 0 & 0 & \cdots \\
\vdots & \vdots & \vdots & \vdots
\end{array}\right]}
\end{array}
$$

We can decompose the final channel $\mathsf{C}^{\mathsf{Lineu}}$ into subchannels, each corresponding to one of the subcomponents (hints and data release): $\mathsf{H}^1 \parallel \mathsf{H}^2 \parallel \mathsf{D}$, where

$$(\mathsf{A} \parallel \mathsf{B})_{x,\langle y,z\rangle} \stackrel{\text{def}}{=} \mathsf{A}_{x,y}\,\mathsf{B}_{x,z}$$

We can decompose the final channel $\mathsf{C}^{\mathsf{Lineu}}$ into subchannels, each corresponding to one of the subcomponents (hints and data release): $\mathsf{H}^1 \parallel \mathsf{H}^2 \parallel \mathsf{D}$, where

$$(\mathsf{A} \parallel \mathsf{B})_{x,\langle y,z\rangle} \stackrel{\text{def}}{=} \mathsf{A}_{x,y}\,\mathsf{B}_{x,z}$$

$$\begin{array}{c} \mathsf{H}^1 \\ x_1 \\ x_2 \\ x_3 \\ x_4 \\ x_5 \\ \vdots \end{array}
\begin{array}{c} \begin{array}{cccccc} \text{Pastry} & \text{Clinic} & \text{Araujo} & \text{Uber} & \text{Ibis} & \cdots \end{array} \\
\begin{bmatrix} \frac{1}{2} & \frac{1}{2} & 0 & 0 & 0 & \cdots \\ 0 & 0 & 1 & 0 & 0 & \cdots \\ 0 & \frac{1}{3} & 0 & \frac{1}{3} & \frac{1}{3} & \cdots \\ 0 & 0 & 0 & 1 & 0 & \cdots \\ 0 & 0 & 0 & 1 & 0 & \cdots \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \end{bmatrix} \end{array}
\parallel
\begin{array}{c} \mathsf{H}^2 \\ x_1 \\ x_2 \\ x_3 \\ x_4 \\ x_5 \\ \vdots \end{array}
\begin{array}{c} \begin{array}{cccc} \text{Araujo} & \text{Transfer} & \text{Pastry} & \cdots \end{array} \\
\begin{bmatrix} 1 & 0 & 0 & \cdots \\ 0 & 1 & 0 & \cdots \\ \frac{1}{2} & 0 & \frac{1}{2} & \cdots \\ 1 & 0 & 0 & \cdots \\ 0 & 1 & 0 & \cdots \\ \vdots & \vdots & \vdots & \vdots \end{bmatrix} \end{array}
\parallel
\begin{array}{c} \mathsf{D} \\ x_1 \\ x_2 \\ x_3 \\ x_4 \\ x_5 \\ \vdots \end{array}
\begin{array}{c} \begin{array}{ccc} d & d_2 & \cdots \end{array} \\
\begin{bmatrix} 1 & 0 & \cdots \\ 1 & 0 & \cdots \\ 1 & 0 & \cdots \\ 1 & 0 & \cdots \\ 1 & 0 & \cdots \\ \vdots & \vdots & \vdots \end{bmatrix} \end{array}$$

- Different adversaries are modelled via gain functions

Formal Model — Modelling Adversaries

- Different adversaries are modelled via gain functions
- A gain function $g : \mathcal{W} \times \mathcal{X} \to \mathbb{R}$ measures the gain of the adversary if they take an action $w \in \mathcal{W}$ when the secret input is some $x \in \mathcal{X}$

Formal Model — Modelling Adversaries

- Different adversaries are modelled via gain functions
- A gain function $g : \mathcal{W} \times \mathcal{X} \to \mathbb{R}$ measures the gain of the adversary if they take an action $w \in \mathcal{W}$ when the secret input is some $x \in \mathcal{X}$
- An adversary who wants to recover the whole secret dataset is modelled as

$$\mathbf{1}(w, x) \stackrel{\text{def}}{=} 1 \text{ if } w = x \text{ else } 0$$

- Different adversaries are modelled via gain functions
- A gain function $g : \mathcal{W} \times \mathcal{X} \to \mathbb{R}$ measures the gain of the adversary if they take an action $w \in \mathcal{W}$ when the secret input is some $x \in \mathcal{X}$
- An adversary who wants to recover the whole secret dataset is modelled as

$$\mathbf{1}(w, x) \stackrel{\text{def}}{=} 1 \text{ if } w = x \text{ else } 0$$

- An adversary with a particular target, say Lineu, is modelled as

$$\mathbf{1}_{\text{Lineu}}(w, x) \stackrel{\text{def}}{=} 1 \text{ if } w = x\texttt{@Lineu} \text{ else } 0,$$

where $x\texttt{@Lineu}$ returns the record labelled as Lineu in x

Formal Model — Quantifying Leakage

- We assume a Bayesian adversary

Formal Model — Quantifying Leakage

- We assume a Bayesian adversary
- The adversary starts with a prior knowledge $\pi : \mathbb{D}\mathcal{X}$

- We assume a Bayesian adversary
- The adversary starts with a prior knowledge $\pi : \mathbb{D}\mathcal{X}$
- Given the prior knowledge, the prior g-vulnerability is

$$V_g(\pi) \stackrel{\text{def}}{=} \max_{w \in \mathcal{W}} \sum_{x \in \mathcal{X}} \pi_x \, g(w, x)$$

Formal Model — **Quantifying Leakage**

- We assume a Bayesian adversary
- The adversary starts with a prior knowledge $\pi : \mathbb{D}\mathcal{X}$
- Given the prior knowledge, the prior g-vulnerability is

$$V_g(\pi) \overset{\text{def}}{=} \max_{w \in \mathcal{W}} \sum_{x \in \mathcal{X}} \pi_x \, g(w, x)$$

- The adversary computes a distribution on the possible outputs as

$$(\pi \triangleright \mathsf{C})_y \overset{\text{def}}{=} \sum_{x \in \mathcal{X}} (\pi \triangleright \mathsf{C})_{x,y} = \sum_{x \in \mathcal{X}} \pi_x \, \mathsf{C}_{x,y}$$

Quantifying Leakage

- We assume a Bayesian adversary
- The adversary starts with a prior knowledge $\pi : \mathbb{D}\mathcal{X}$
- Given the prior knowledge, the prior g-vulnerability is

$$V_g(\pi) \stackrel{\text{def}}{=} \max_{w \in \mathcal{W}} \sum_{x \in \mathcal{X}} \pi_x \, g(w, x)$$

- The adversary computes a distribution on the possible outputs as

$$(\pi \triangleright \mathsf{C})_y \stackrel{\text{def}}{=} \sum_{x \in \mathcal{X}} (\pi \triangleright \mathsf{C})_{x,y} = \sum_{x \in \mathcal{X}} \pi_x \, \mathsf{C}_{x,y}$$

- And distributions on the possible secret values, conditioned on outputs, as

$$(\pi \triangleright \mathsf{C})_{x|y} \stackrel{\text{def}}{=} \frac{(\pi \triangleright \mathsf{C})_{x,y}}{(\pi \triangleright \mathsf{C})_y} = \frac{\pi_x \, \mathsf{C}_{x,y}}{(\pi \triangleright \mathsf{C})_y}$$

- Then, the (expected) posterior g-vulnerability is

$$V_g[\pi \triangleright \mathsf{C}] \stackrel{\text{def}}{=} \sum_{y \in \mathcal{Y}} (\pi \triangleright \mathsf{C})_y \, V_g((\pi \triangleright \mathsf{C})_{X|y})$$

- Then, the (expected) posterior g-vulnerability is

$$V_g[\pi \triangleright \mathrm{C}] \stackrel{\text{def}}{=} \sum_{y \in \mathcal{Y}} (\pi \triangleright \mathrm{C})_y \, V_g((\pi \triangleright \mathrm{C})_{X|y})$$

- And the information that leaks in the attack can be measured (multiplicatively) as

$$\mathcal{L}_g(\pi, \mathrm{C}) \stackrel{\text{def}}{=} \frac{V_g[\pi \triangleright \mathrm{C}]}{V_g(\pi)}$$

Formal Model — Quantifying Leakage

- Then, the (expected) posterior g-vulnerability is

$$V_g[\pi \triangleright \mathrm{C}] \stackrel{\text{def}}{=} \sum_{y \in \mathcal{Y}} (\pi \triangleright \mathrm{C})_y \, V_g((\pi \triangleright \mathrm{C})_{X|y})$$

- And the information that leaks in the attack can be measured (multiplicatively) as

$$\mathcal{L}_g(\pi, \mathrm{C}) \stackrel{\text{def}}{=} \frac{V_g[\pi \triangleright \mathrm{C}]}{V_g(\pi)}$$

- In our running example, $g = \mathbf{1}_{\mathrm{Lineu}}$ and $\mathrm{C} = \mathrm{C}^{\mathrm{Lineu}} = \mathrm{H}^1 \parallel \mathrm{H}^2 \parallel \mathrm{D}$

Formal Model — Quantifying Leakage

$$
\begin{array}{c}
\pi \\
\begin{array}{c} x_1 \\ x_2 \\ x_3 \\ x_4 \\ x_5 \\ \vdots \end{array}
\begin{bmatrix} \frac{1}{|\mathcal{X}|} \\ \frac{1}{|\mathcal{X}|} \\ \frac{1}{|\mathcal{X}|} \\ \frac{1}{|\mathcal{X}|} \\ \frac{1}{|\mathcal{X}|} \\ \vdots \end{bmatrix}
\end{array}
[\triangleright]
\begin{array}{c}
\mathsf{C}^{\mathsf{Lineu}} \quad \langle \text{Pastry}, \text{Araujo}, d\rangle \ \langle \text{Clinic}, \text{Araujo}, d\rangle \ \cdots \\
\begin{array}{c} x_1 \\ x_2 \\ x_3 \\ x_4 \\ x_5 \\ \vdots \end{array}
\begin{bmatrix} \frac{1}{2} & \frac{1}{2} & \cdots \\ 0 & 0 & \cdots \\ 0 & \frac{1}{6} & \cdots \\ 0 & 0 & \cdots \\ 0 & 0 & \cdots \\ \vdots & \vdots & \vdots \end{bmatrix}
\end{array}
=
\begin{array}{c}
\frac{4!}{2|\mathcal{X}|} \langle \text{Pastry}, \text{Araujo}, d\rangle \ \frac{2\cdot 4!}{3|\mathcal{X}|} \langle \text{Clinic}, \text{Araujo}, d\rangle \ \cdots \\
\begin{array}{c} x_1 \\ x_2 \\ x_3 \\ x_4 \\ x_5 \\ \vdots \end{array}
\begin{bmatrix} \frac{1}{4!} & \frac{3}{4\cdot 4!} & \cdots \\ 0 & 0 & \cdots \\ 0 & \frac{1}{4\cdot 4!} & \cdots \\ 0 & 0 & \cdots \\ 0 & 0 & \cdots \\ \vdots & \vdots & \vdots \end{bmatrix}
\end{array}
$$

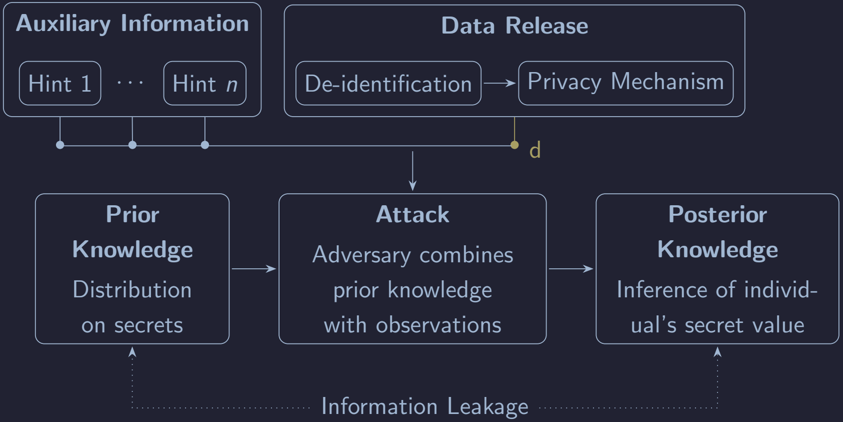
Formal Model — Quantifying Leakage

$$
\begin{array}{cc}
\pi & \\
\begin{array}{c} x_1 \\ x_2 \\ x_3 \\ x_4 \\ x_5 \\ \vdots \end{array} &
\begin{bmatrix} \frac{1}{|\mathcal{X}|} \\ \frac{1}{|\mathcal{X}|} \\ \frac{1}{|\mathcal{X}|} \\ \frac{1}{|\mathcal{X}|} \\ \frac{1}{|\mathcal{X}|} \\ \vdots \end{bmatrix}
\end{array}
[\triangleright]
\begin{array}{cc}
\mathsf{C}^{\mathsf{Lineu}} & \begin{array}{ccc} \langle \text{Pastry, Araujo}, d \rangle & \langle \text{Clinic, Araujo}, d \rangle & \cdots \end{array} \\
\begin{array}{c} x_1 \\ x_2 \\ x_3 \\ x_4 \\ x_5 \\ \vdots \end{array} &
\begin{bmatrix} \frac{1}{2} & \frac{1}{2} & \cdots \\ 0 & 0 & \cdots \\ 0 & \frac{1}{6} & \cdots \\ 0 & 0 & \cdots \\ 0 & 0 & \cdots \\ \vdots & \vdots & \vdots \end{bmatrix}
\end{array}
=
\begin{array}{cc}
 & \begin{array}{ccc} \frac{4!}{2|\mathcal{X}|}\,\langle \text{Pastry, Araujo}, d \rangle & \frac{2\cdot 4!}{3|\mathcal{X}|}\,\langle \text{Clinic, Araujo}, d \rangle & \cdots \end{array} \\
\begin{array}{c} x_1 \\ x_2 \\ x_3 \\ x_4 \\ x_5 \\ \vdots \end{array} &
\begin{bmatrix} \frac{1}{4!} & \frac{3}{4\cdot 4!} & \cdots \\ 0 & 0 & \cdots \\ 0 & \frac{1}{4\cdot 4!} & \cdots \\ 0 & 0 & \cdots \\ 0 & 0 & \cdots \\ \vdots & \vdots & \vdots \end{bmatrix}
\end{array}
$$

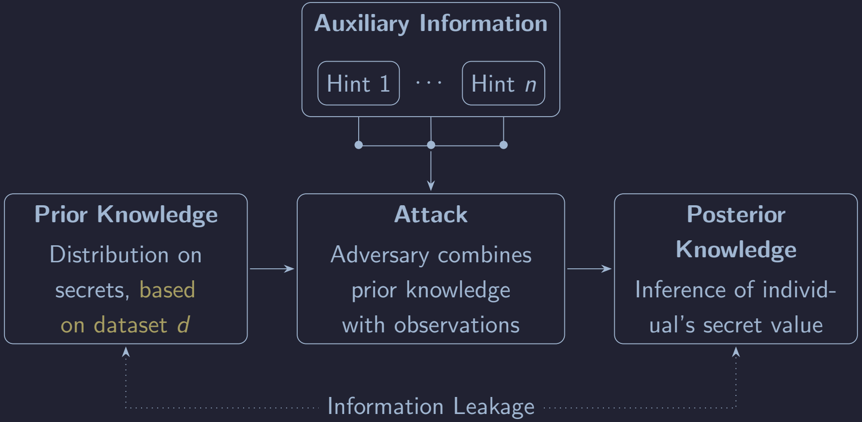
There are 4! datasets similar to x_1, in which Lineu's record is $\vec{t}_1$, so

$$(\pi \triangleright \mathsf{C}^{\mathsf{Lineu}})_{\langle \text{Pastry,Araujo},d \rangle} = {}^{4!}/(2|\mathcal{X}|)$$

We cannot compute over all possible de-identified datasets that could be released, so we focus on one particular dataset d, assuming the adversary has already observed it:



We cannot compute over all possible de-identified datasets that could be released, so we focus on one particular dataset d, assuming the adversary has already observed it:



Formal Model — Simplified Model — Secrets

In our experiments, there are no two customers with the same transaction history. So, we can group secrets that are "similar". For instance, every dataset that maps to d in which Lineu's record is $\vec{t}_1$. Then, the space of secrets becomes the transaction histories:

$$
\begin{array}{c}
\upsilon \\
\begin{array}{c} \vec{t}_1 \\ \vec{t}_2 \\ \vec{t}_3 \\ \vec{t}_4 \\ \vec{t}_5 \end{array}
\left[\begin{array}{c} \frac{1}{5} \\ \frac{1}{5} \\ \frac{1}{5} \\ \frac{1}{5} \\ \frac{1}{5} \end{array}\right]
\end{array}
[\triangleright]
\begin{array}{c}
\mathsf{C}^{\mathsf{Lineu}} \quad \langle \text{Pastry, Araujo} \rangle \ \langle \text{Clinic, Araujo} \rangle \ \cdots \\
\begin{array}{c} \vec{t}_1 \\ \vec{t}_2 \\ \vec{t}_3 \\ \vec{t}_4 \\ \vec{t}_5 \end{array}
\left[\begin{array}{ccc} \frac{1}{2} & \frac{1}{2} & \cdots \\ 0 & 0 & \cdots \\ 0 & \frac{1}{6} & \cdots \\ 0 & 0 & \cdots \\ 0 & 0 & \cdots \end{array}\right]
\end{array}
=
\begin{array}{c}
\frac{1}{10} \langle \text{Pastry, Araujo} \rangle \ \frac{2}{15} \langle \text{Clinic, Araujo} \rangle \ \cdots \\
\begin{array}{c} \vec{t}_1 \\ \vec{t}_2 \\ \vec{t}_3 \\ \vec{t}_4 \\ \vec{t}_5 \end{array}
\left[\begin{array}{ccc} 1 & \frac{3}{4} & \cdots \\ 0 & 0 & \cdots \\ 0 & \frac{1}{4} & \cdots \\ 0 & 0 & \cdots \\ 0 & 0 & \cdots \end{array}\right]
\end{array}
$$

In our experiments, there are no two customers with the same transaction history. So, we can group secrets that are “similar”. For instance, every dataset that maps to d in which Lineu's record is $\vec{t}_1$. Then, the space of secrets becomes the transaction histories:

$$
\begin{array}{c}
\upsilon \\
\begin{array}{c}\vec{t}_1\\ \vec{t}_2\\ \vec{t}_3\\ \vec{t}_4\\ \vec{t}_5\end{array}
\begin{bmatrix} \frac{1}{5} \\ \frac{1}{5} \\ \frac{1}{5} \\ \frac{1}{5} \\ \frac{1}{5} \end{bmatrix}
\end{array}
[\triangleright]
\begin{array}{cc}
\mathsf{C}^{\mathsf{Lineu}} & \begin{array}{ccc} \langle \text{Pastry, Araujo} \rangle & \langle \text{Clinic, Araujo} \rangle & \cdots \end{array} \\
\begin{array}{c}\vec{t}_1\\ \vec{t}_2\\ \vec{t}_3\\ \vec{t}_4\\ \vec{t}_5\end{array} &
\begin{bmatrix}
\frac{1}{2} & \frac{1}{2} & \cdots \\
0 & 0 & \cdots \\
0 & \frac{1}{6} & \cdots \\
0 & 0 & \cdots \\
0 & 0 & \cdots
\end{bmatrix}
\end{array}
=
\begin{array}{cc}
 & \begin{array}{ccc} \frac{1}{10}\,\langle \text{Pastry, Araujo} \rangle & \frac{2}{15}\,\langle \text{Clinic, Araujo} \rangle & \cdots \end{array} \\
\begin{array}{c}\vec{t}_1\\ \vec{t}_2\\ \vec{t}_3\\ \vec{t}_4\\ \vec{t}_5\end{array} &
\begin{bmatrix}
1 & \frac{3}{4} & \cdots \\
0 & 0 & \cdots \\
0 & \frac{1}{4} & \cdots \\
0 & 0 & \cdots \\
0 & 0 & \cdots
\end{bmatrix}
\end{array}
$$

and the gain function $\mathbf{1}_{\mathsf{Lineu}}$ is replaced with $\mathbf{1}$

$$\begin{array}{cc} & \begin{array}{cccc} \frac{1}{10}\,\langle \text{Pastry, Araujo}\rangle & \frac{2}{15}\,\langle \text{Clinic, Araujo}\rangle & \frac{1}{30}\,\langle \text{Clinic, Pastry}\rangle & \cdots \end{array} \\ \begin{array}{c} \vec{t}_1 \\ \vec{t}_2 \\ \vec{t}_3 \\ \vec{t}_4 \\ \vec{t}_5 \end{array} & \begin{bmatrix} 1 & \frac{3}{4} & 0 & \cdots \\ 0 & 0 & 0 & \cdots \\ 0 & \frac{1}{4} & 1 & \cdots \\ 0 & 0 & 0 & \cdots \\ 0 & 0 & 0 & \cdots \end{bmatrix} \end{array}$$

$$\begin{array}{c} \\ \vec{t}_1 \\ \vec{t}_2 \\ \vec{t}_3 \\ \vec{t}_4 \\ \vec{t}_5 \end{array} \begin{array}{c} \begin{array}{cccc} \frac{1}{10}\langle \text{Pastry}, \text{Araujo}\rangle & \frac{2}{15}\langle \text{Clinic}, \text{Araujo}\rangle & \frac{1}{30}\langle \text{Clinic}, \text{Pastry}\rangle & \cdots \end{array} \\ \begin{bmatrix} 1 & \frac{3}{4} & 0 & \cdots \\ 0 & 0 & 0 & \cdots \\ 0 & \frac{1}{4} & 1 & \cdots \\ 0 & 0 & 0 & \cdots \\ 0 & 0 & 0 & \cdots \end{bmatrix} \end{array}$$

- The prior vulnerability is then $V_{\mathbf{1}}(v) = {}^{1}\!/_{5}$

$$\begin{array}{c|cccc} & \frac{1}{10}\,\langle \text{Pastry}, \text{Araujo}\rangle & \frac{2}{15}\,\langle \text{Clinic}, \text{Araujo}\rangle & \frac{1}{30}\,\langle \text{Clinic}, \text{Pastry}\rangle & \cdots \\ \hline \vec{t}_1 & 1 & \frac{3}{4} & 0 & \cdots \\ \vec{t}_2 & 0 & 0 & 0 & \cdots \\ \vec{t}_3 & 0 & \frac{1}{4} & 1 & \cdots \\ \vec{t}_4 & 0 & 0 & 0 & \cdots \\ \vec{t}_5 & 0 & 0 & 0 & \cdots \end{array}$$

- The prior vulnerability is then $V_{\mathbf{1}}(\upsilon) = {}^{1}\!/_{5}$
- The posterior vulnerability is $V_{\mathbf{1}}[\upsilon \triangleright \mathsf{C}^{\mathsf{Lineu}}] = {}^{1}\!/_{10} + {}^{2}\!/_{15} \cdot {}^{3}\!/_{4} + {}^{1}\!/_{30} + \cdots = {}^{14}\!/_{15}$

$$
\begin{array}{c|cccc}
 & \frac{1}{10}\,\langle \text{Pastry}, \text{Araujo}\rangle & \frac{2}{15}\,\langle \text{Clinic}, \text{Araujo}\rangle & \frac{1}{30}\,\langle \text{Clinic}, \text{Pastry}\rangle & \cdots \\
\vec{t}_1 & 1 & \frac{3}{4} & 0 & \cdots \\
\vec{t}_2 & 0 & 0 & 0 & \cdots \\
\vec{t}_3 & 0 & \frac{1}{4} & 1 & \cdots \\
\vec{t}_4 & 0 & 0 & 0 & \cdots \\
\vec{t}_5 & 0 & 0 & 0 & \cdots
\end{array}
$$

- The prior vulnerability is then $V_{\mathbf{1}}(\upsilon) = {}^{1}\!/_{5}$
- The posterior vulnerability is $V_{\mathbf{1}}[\upsilon \triangleright \mathsf{C}^{\mathsf{Lineu}}] = {}^{1}\!/_{10} + {}^{2}\!/_{15} \cdot {}^{3}\!/_{4} + {}^{1}\!/_{30} + \cdots = {}^{14}\!/_{15}$
- The information that leaks in this attack is thus $\mathcal{L}_{\mathbf{1}}(\upsilon, \mathsf{C}^{\mathsf{Lineu}}) = {}^{14}\!/_{3} \approx 4.67$

Conclusion & Future Work

- We developed a formal model for attacks against data releases, with a case study in which we analysed the implementation of Open Banking (in Australia)

Conclusion & Future Work

- We developed a formal model for attacks against data releases, with a case study in which we analysed the implementation of Open Banking (in Australia)
- We highlighted the risks of data sharing for consumers, for both transaction-history recovery and indirect attribute-inference risks (see paper)

Conclusion & Future Work

- We developed a formal model for attacks against data releases, with a case study in which we analysed the implementation of Open Banking (in Australia)
- We highlighted the risks of data sharing for consumers, for both transaction-history recovery and indirect attribute-inference risks (see paper)
- This is an ongoing research. We are currently working on the analysis of privacy mechanisms, and this led us to discover a gap in the literature when considering dynamic scenarios (i.e., fixed outputs)

Conclusion & Future Work

- We developed a formal model for attacks against data releases, with a case study in which we analysed the implementation of Open Banking (in Australia)
- We highlighted the risks of data sharing for consumers, for both transaction-history recovery and indirect attribute-inference risks (see paper)
- This is an ongoing research. We are currently working on the analysis of privacy mechanisms, and this led us to discover a gap in the literature when considering dynamic scenarios (i.e., fixed outputs)
- This project has recently resulted in a grant from the Australian Research Council (ARC), under the 2025 Discovery Projects program!