Understanding Information Disclosure from Secure Computation Output: A Study of Average Salary Computation

Alessandro Baccarini, Marina Blanton, Shaofeng Zou

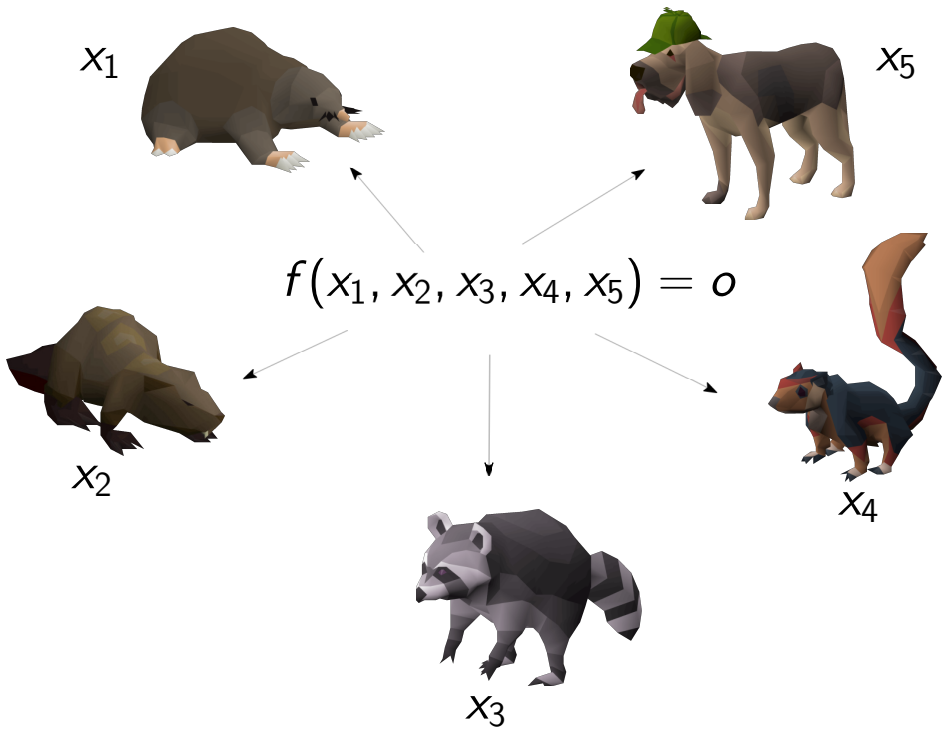
Department of Computer Science and Engineering
University at Buffalo

{anbaccar,mblanton,szou3}@buffalo.edu

June 20, 2024

Table of Contents

What *is* secure (multi-party) computation?

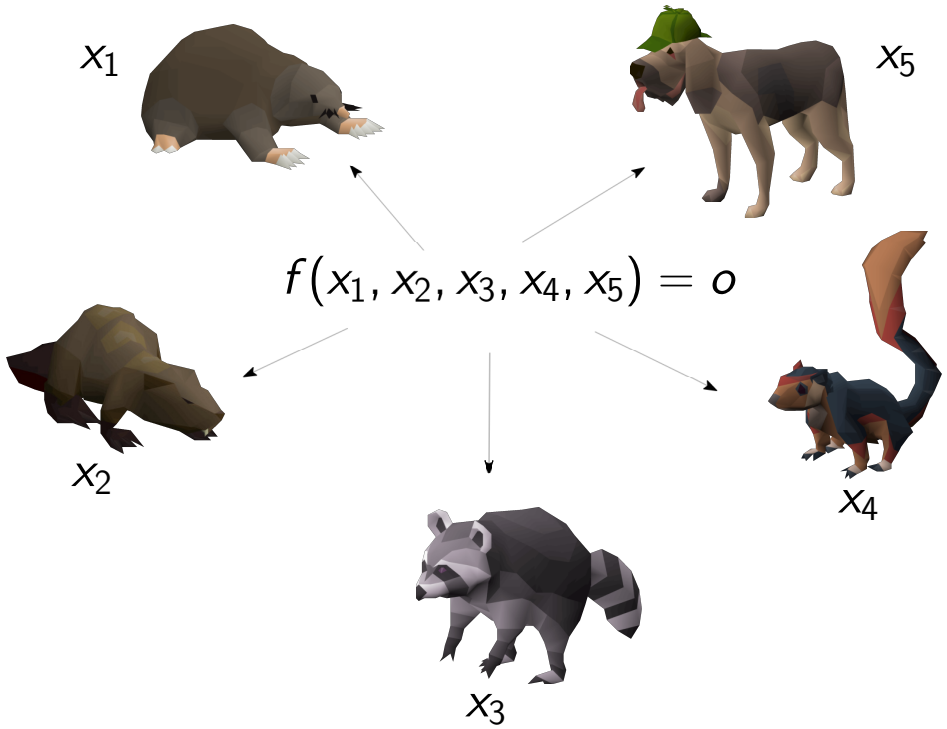


Secure multi-party computation (SMC)

Multiple participants jointly evaluating a function on secret inputs

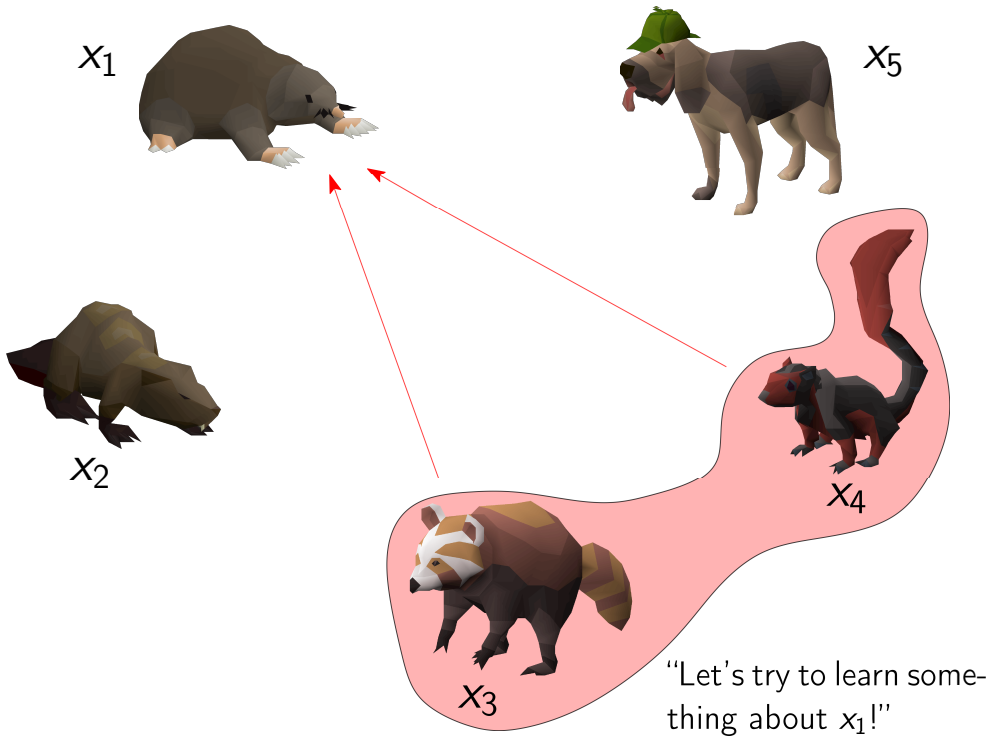
- **No information is disclosed other than the output**
- Variety of practical applications

Broader questions about secure computation



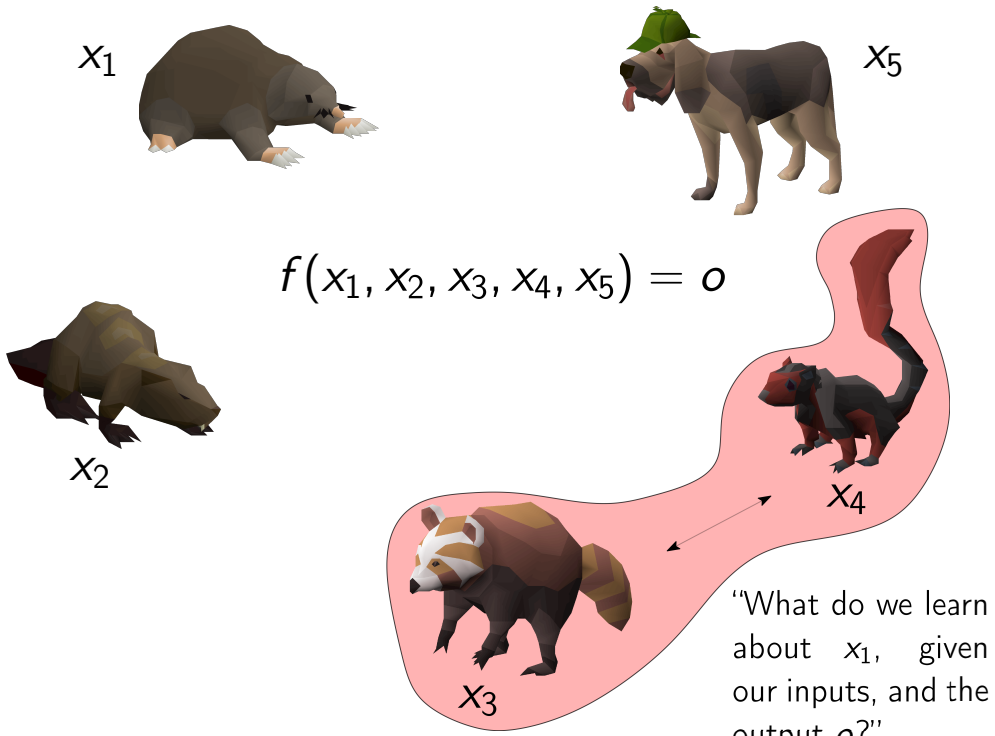
- What can happen **after** the function is evaluated?
- Does the **output itself** leak any sensitive information?
- Can we **quantify** this disclosure?

Broader questions about secure computation



- What can happen **after** the function is evaluated?
- Does the **output itself** leak any sensitive information?
- Can we **quantify** this disclosure?

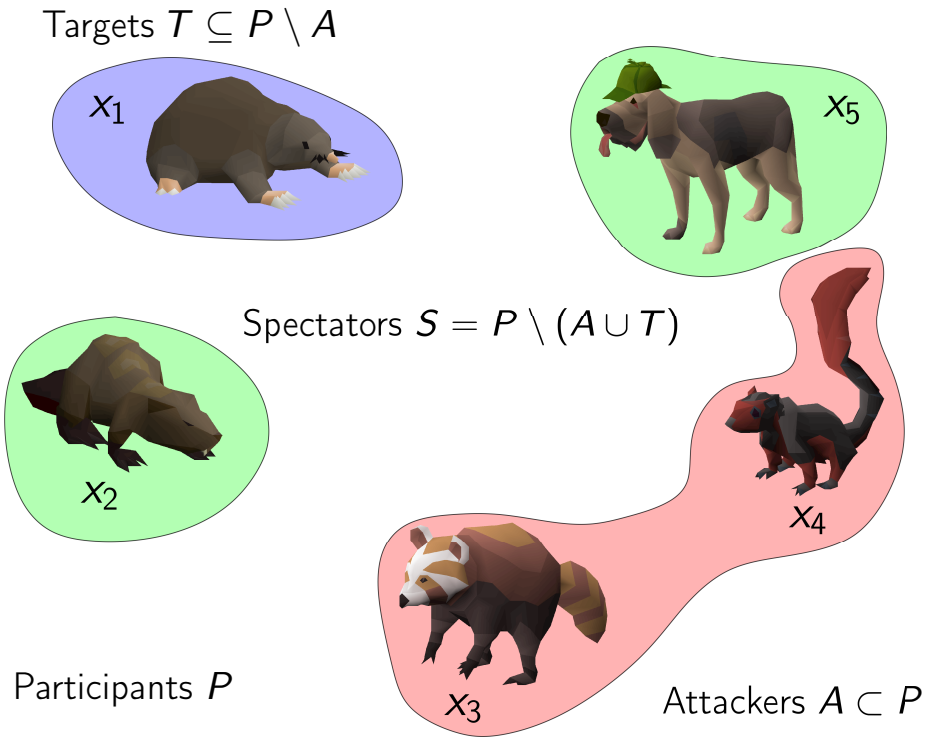
Broader questions about secure computation



- What can happen **after** the function is evaluated?
- Does the **output itself** leak any sensitive information?
- Can we **quantify** this disclosure?

Setting

– How do we differentiate participants from one another?



Metric?

- Model participant i's input by a random variable X_{P_i}
- How should we **measure** the **information** disclosed from the output?

Metric?

- Model participant i's input by a random variable X_{P_i}
- How should we **measure** the **information** disclosed from the output?

Entropy!

Metric?

- Model participant i's input by a random variable X_{P_i}
- How should we **measure** the **information** disclosed from the output?

Entropy!

Shannon (discrete)

$$H(X) = -\sum_{x \in \mathcal{X}} \Pr(X = x) \log \Pr(X = x)$$

Differential (continuous)

$$h(X) = -\int_{\mathcal{X}} f(x) \log f(x) dx$$

Putting it together

- Attackers $\vec{X}_A$, targets $\vec{X}_T$ spectators $\vec{X}_S$
- Treat the **output** as a random variable:

$$f(\vec{X}_A, \vec{X}_T, \vec{X}_S) = X_A + X_T + X_S = O$$

Attackers' weighted average entropy[1]

$H(\vec{X}_T \mid \vec{X}_A = \vec{x}_A, O) \implies$ how much information is learned about the target, given $\vec{x}_A$ and O

- Equivalent expression for differential entropy

[1] P. Ah-Fat and M. Huth. "Secure Multi-party Computation: Information Flow of Outputs and Game Theory". In: *International Conference on Principles of Security and Trust*. 2017, pp. 71–92

Where to begin?

- 2016 Boston gender pay gap survey[2]
- Analyzed the **private** wages based on gender and race **using SMC**
- **Average salary computation**

Mayor Walsh & Boston Women's Workforce Council Release 2016 Gender Wage Gap Report; New Partnership with BU

Thursday, January 5, 2017 – Mayor Martin J. Walsh and the Boston Women's Workforce Council (BWWC) released the 2016 gender wage report and announced a new academic partnership with Boston University, where the BWWC will now be hosted within the BU Hariri Institute for Computing.

Source: Boston University, 2017

- Average $\implies$ reduces to a **sum**:

$$f_\mu(\vec{x}) = \frac{1}{n}(x_1 + x_2 + \cdots + x_n) \implies x_1 + x_2 + \cdots + x_n$$

[2] Boston Women's Workforce Council. *Boston Women's Workforce Council Report 2016*. link. 2017

Where to begin?

- 2016 Boston gender pay gap survey[2]
- Analyzed the **private** wages based on gender and race **using SMC**
- **Average salary computation**

Mayor Walsh & Boston Women's Workforce Council Release 2016 Gender Wage Gap Report; New Partnership with BU

Thursday, January 5, 2017 – Mayor Martin J. Walsh and the Boston Women's Workforce Council (BWWC) released the 2016 gender wage report and announced a new academic partnership with Boston University, where the BWWC will now be hosted within the BU Hariri Institute for Computing.

Source: Boston University, 2017

- Average $\implies$ reduces to a **sum**:

$$f_\mu(\vec{x}) = \frac{1}{n}\left(x_1 + x_2 + \cdots + x_n\right) \implies \boxed{x_1 + x_2 + \cdots + x_n}$$

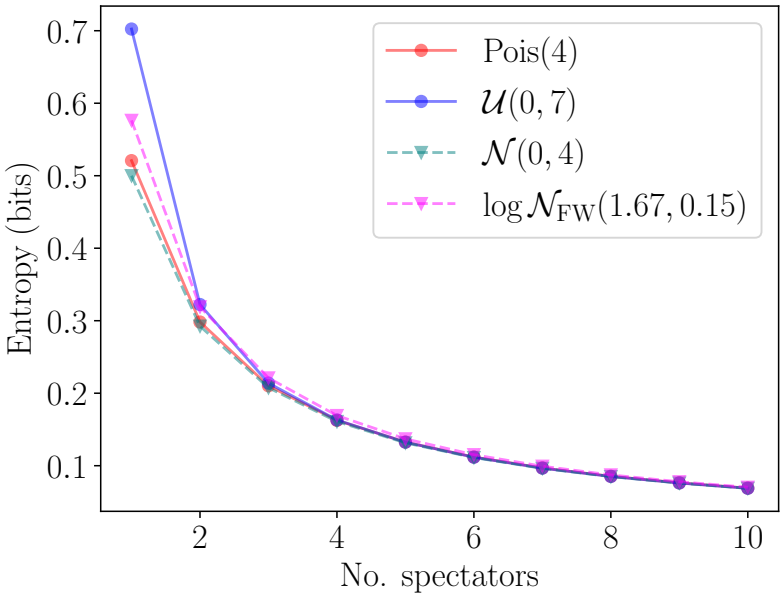
[2] Boston Women's Workforce Council. *Boston Women's Workforce Council Report 2016*. link. 2017

Single evaluation

- Information disclosure is **independent** of:
  - the attackers' input(s) $\implies H(\vec{X}_T \mid \vec{X}_A = \vec{x}_A, O) = H(\vec{X}_T \mid O)$

$$O = X_T + X_S + X_A \text{ “} = \text{” } X_T + X_S$$

  - the input distribution (Poisson, uniform, **Gaussian**, log-normal[3]) and its parameters



Absolute loss
= Target's initial entropy
− remaining entropy

- Entropy loss is proportional to the number of spectators

[3] F. Clementi and M. Gallegati. "Pareto's Law of Income Distribution: Evidence for Germany, the United Kingdom, and the United States". In: *Econophysics of Wealth Distributions*. Springer, 2005, pp. 3–14. DOI: 10.1007/88-470-0389-X_1.

Two evaluations

- Does the wage gap change over time?
- That's what the BWWC wanted to find out![4]

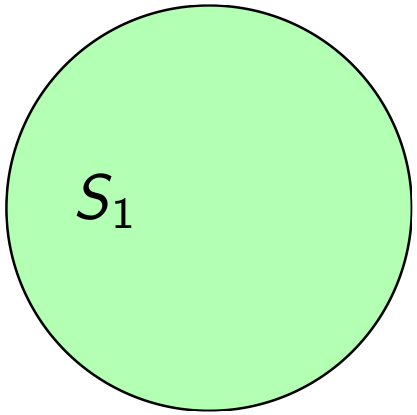
Mayor Walsh & BWWC Release 2017 Wage Gap Report

The Boston Women's Workforce Council released its 2017 report this morning, which uses real employer wage information to assess the pay gap in Boston. The 2017 report

BOSTON WOMEN'S WORKFORCE COUNCIL REPORT 2017

Source: Boston University, 2018

- Spectators present in the first, second, and both evaluation(s)



[4] Boston Women's Workforce Council. *Boston Women's Workforce Council Report 2017*. link. 2018

Two evaluations

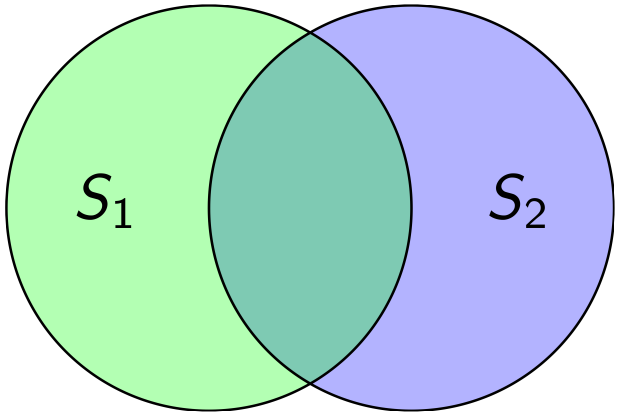
- Does the wage gap change over time?
- That's what the BWWC wanted to find out![4]

Mayor Walsh & BWWC Release 2017 Wage Gap Report

The Boston Women's Workforce Council released its 2017 report this morning, which uses real employer wage information to assess the pay gap in Boston. The 2017 report

BOSTON WOMEN'S WORKFORCE COUNCIL REPORT 2017

Source: Boston University, 2018



- Spectators present in the first, second, and both evaluation(s)

[4] Boston Women's Workforce Council. *Boston Women's Workforce Council Report 2017*. link. 2018

Two evaluations

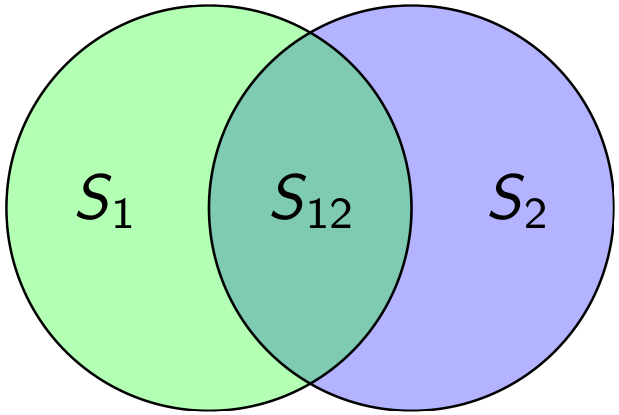
- Does the wage gap change over time?
- That's what the BWWC wanted to find out![4]

Mayor Walsh & BWWC Release 2017 Wage Gap Report

The Boston Women's Workforce Council released its 2017 report this morning, which uses real employer wage information to assess the pay gap in Boston. The 2017 report

BOSTON WOMEN'S WORKFORCE COUNCIL REPORT 2017

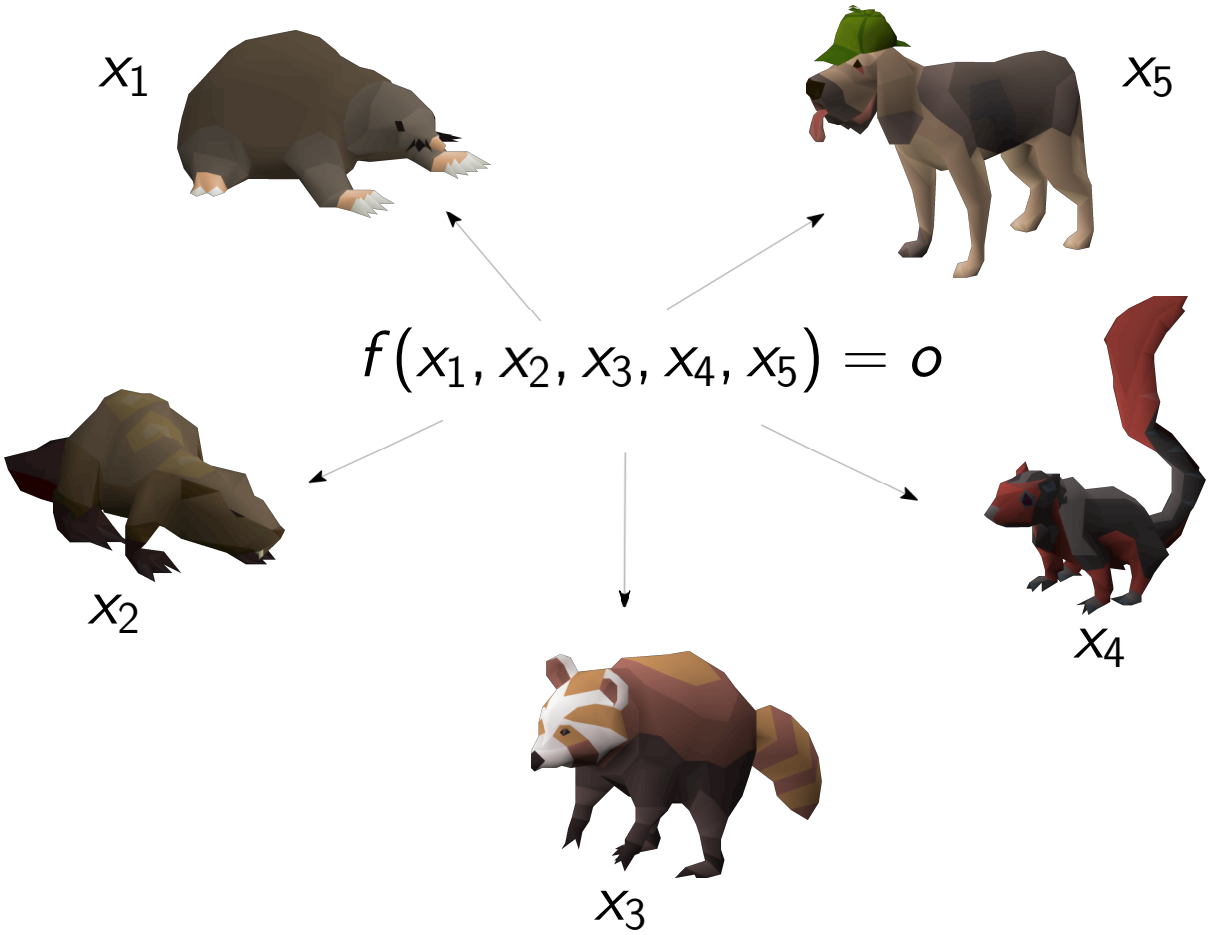
Source: Boston University, 2018



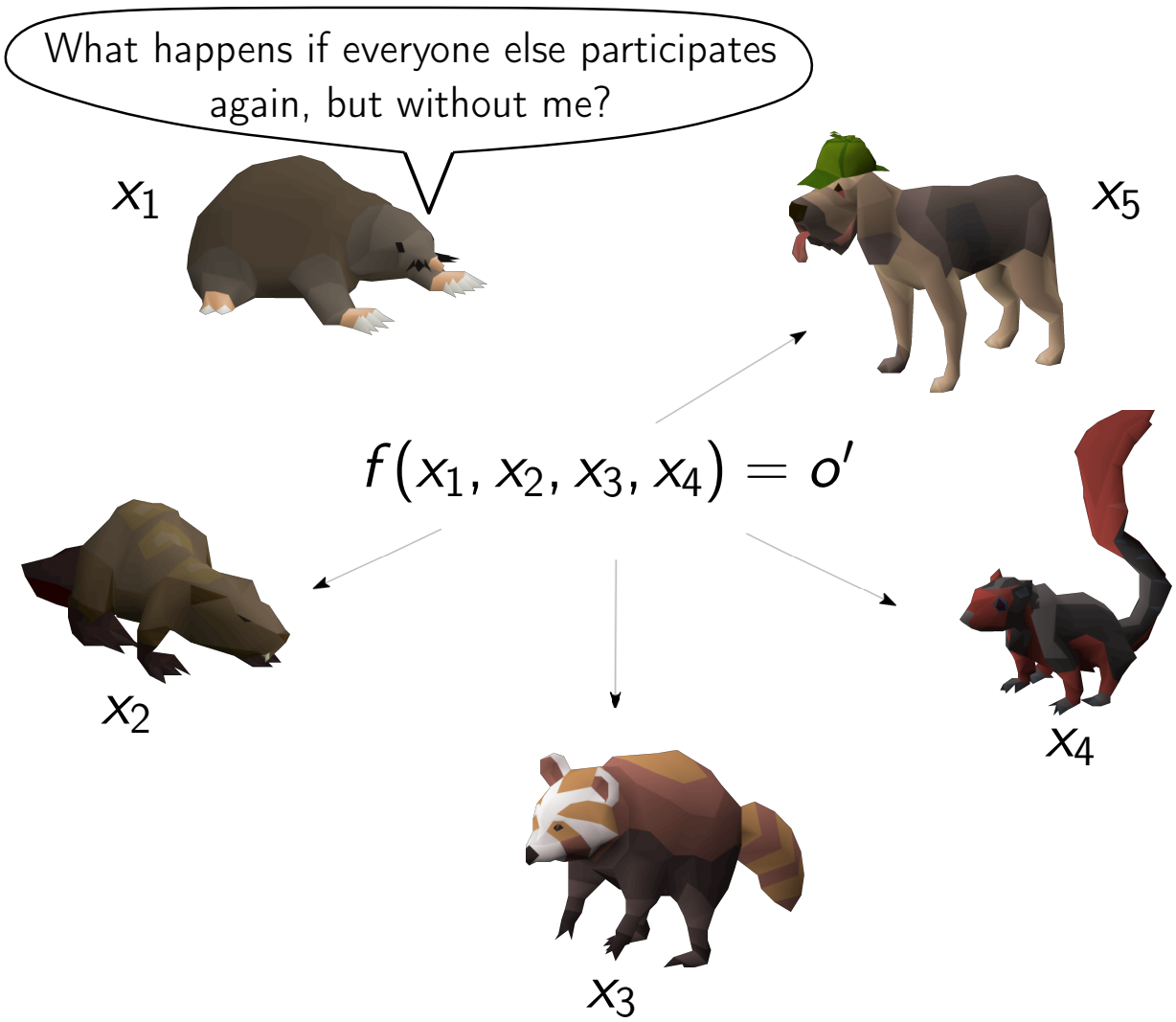
- Spectators present in the first, second, and both evaluation(s)

[4] Boston Women's Workforce Council. *Boston Women's Workforce Council Report 2017*. link. 2018

Two evaluations

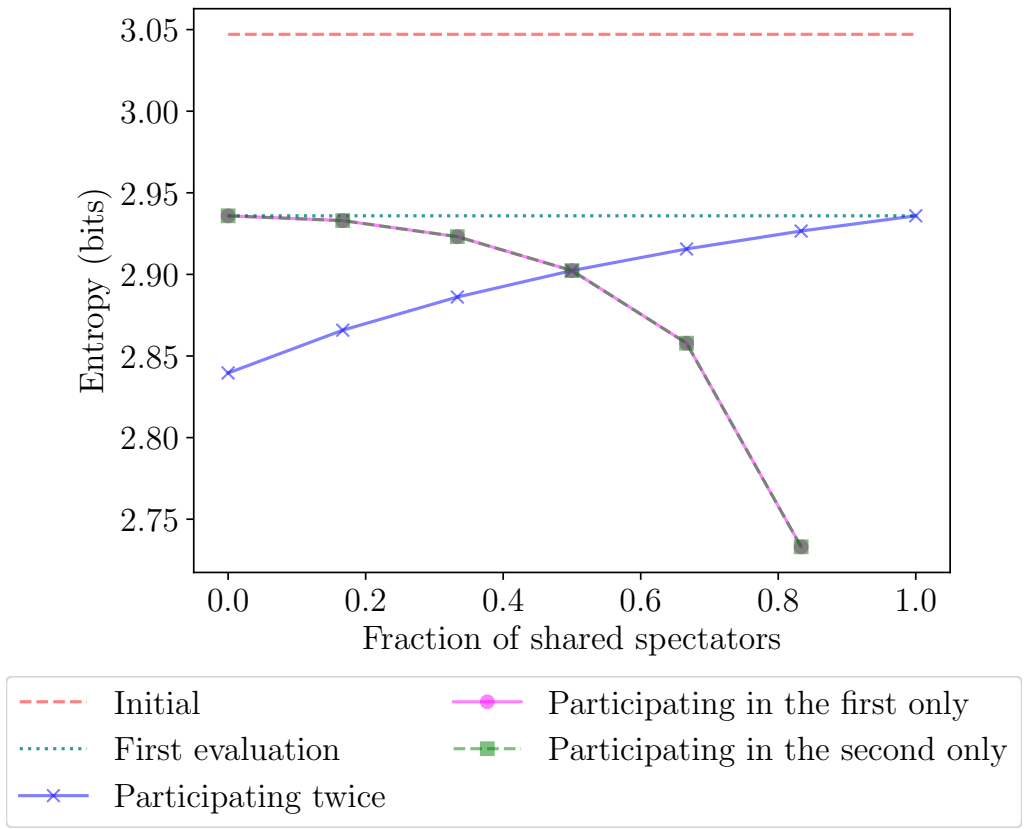


Two evaluations



Two evaluations

- Participating **once** vs. **twice**
- Largest protection at **50% overlap**
- Undesirable disclosure at extrema



Conclusions and future directions

- Analyzed disclosure from output of the average salary
- **Recommendations** for computation designers
- Additional analysis and experiments in full version
  - Three executions and beyond
  - Non-identical input distributions
  - Alternate metric $\implies$ min-entropy
- Advanced descriptive statistics
  - Max/min
  - Median
  - Standard deviation (variance)

Thank you!

Questions?