# Course Announcements

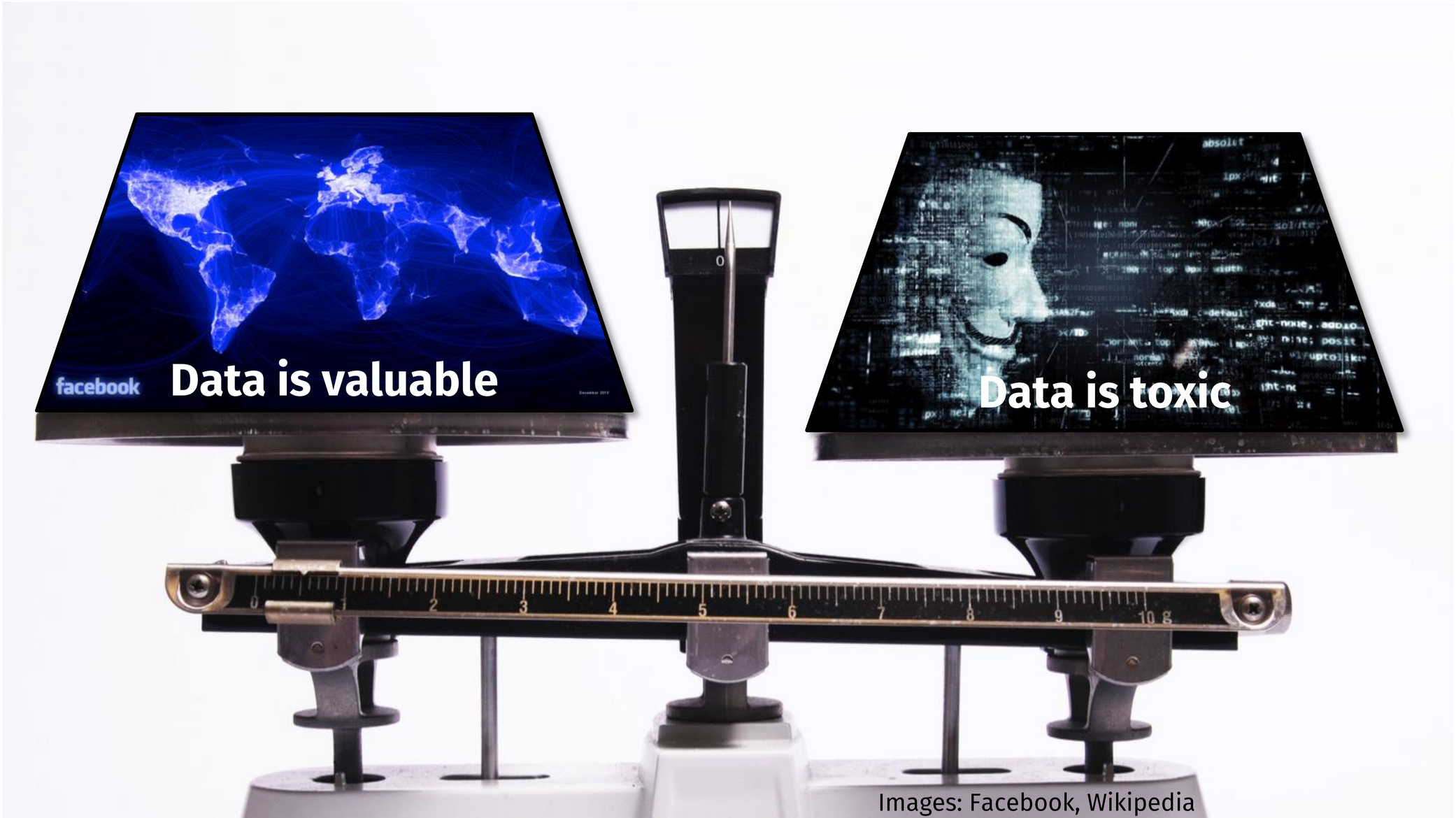
- Assignments
  - Homework 8 is due Wednesday 4/1 and Homework 9 is due 4/8
  - Class project has been posted (see Piazza post 302), due Wednesday 4/22
  - Reading: Secure Multiparty Computation for Privacy-Preserving Data Mining
- Schedule
  - 2 weeks on protecting data in use, including a guest lecture by Ari Trachtenberg
  - 2 weeks on cipher design and cryptanalysis
  - 1 week on cryptography and the law: guest lectures by Andy Sellars

# Lecture 17: Protecting Data in Use

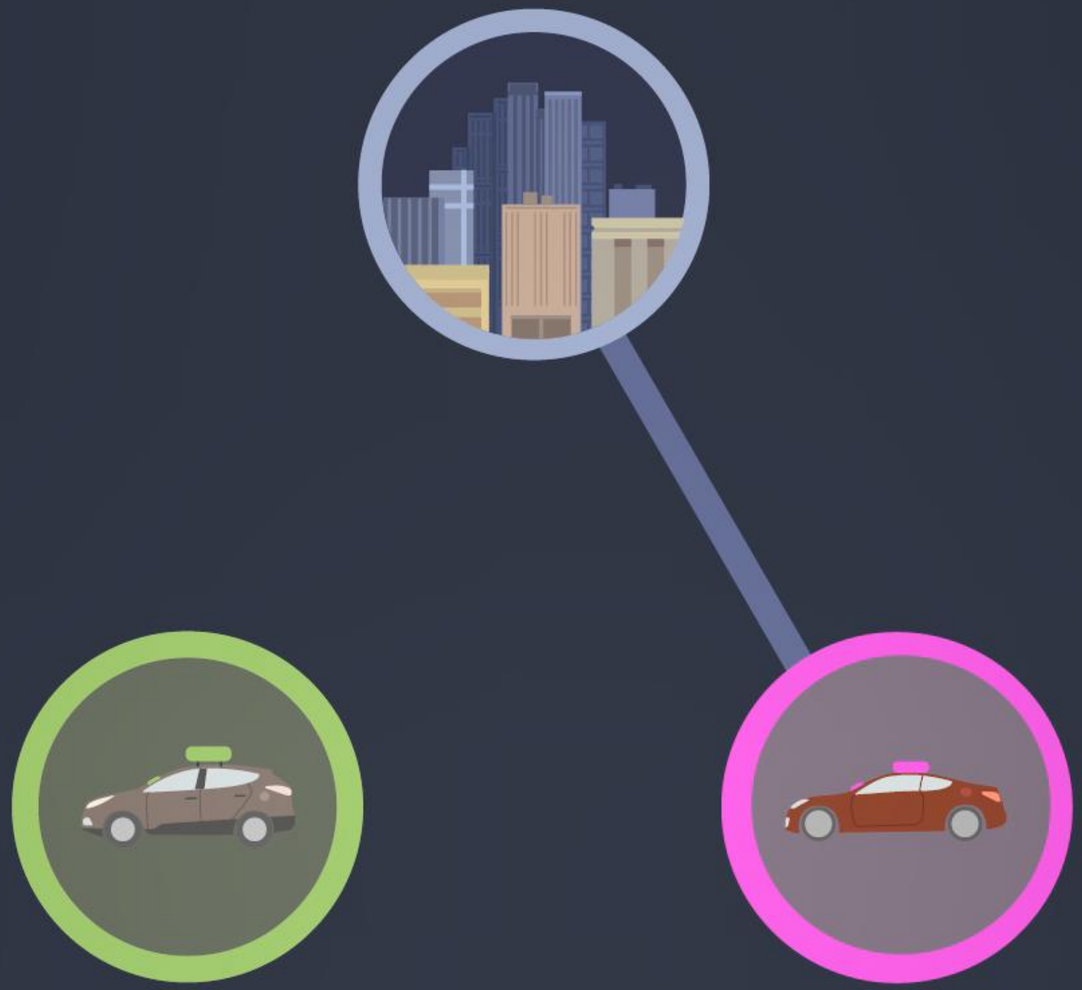
1. Overview
2. An example
3. Securely computing linear functions
4. Secure multiplication
5. Generic secure computation

# 1. Overview

# Oblivious computing




Images: Facebook, Wikipedia

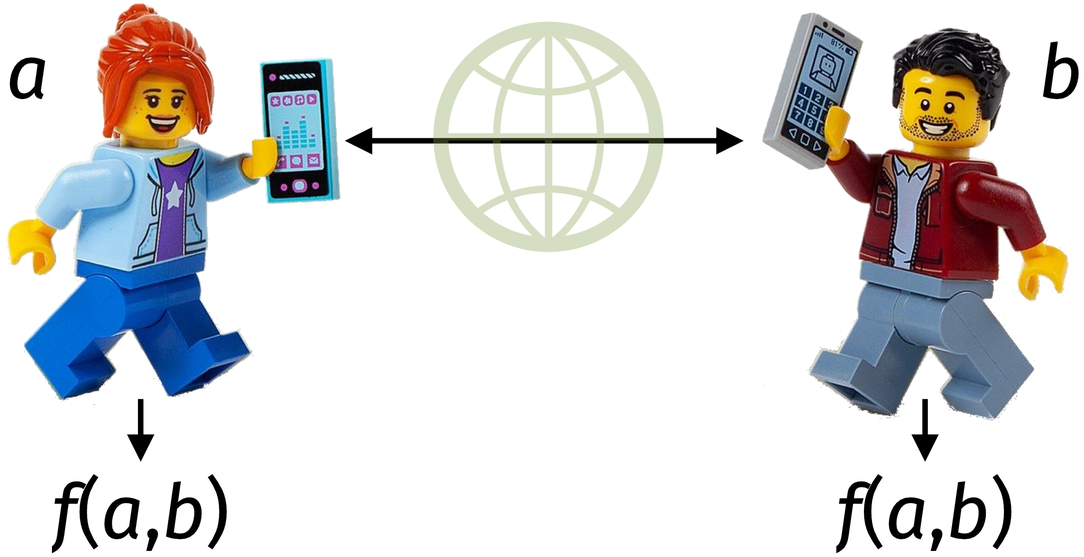


THIS IS SECURE

MULTIPARTY COMPUTATION

# Defining MPC (2019 U.S. Senate bill S.681)

"Secure multi-party computation … enables *different participating entities* in possession of private sets of data to *link and aggregate their data sets* for the exclusive purpose of performing a finite number of pre-approved computations *without transferring or otherwise revealing any private data* to each other or anyone else."



# Objective of secure multi-party computation (MPC)

- Given multiple parties $P_1$, $P_2$, …, $P_n$ each with private data $x_1$, $x_2$, …, $x_n$
- Parties engage in computing a function $y = f(x_1, x_2, \ldots, x_n)$
- Assume that threshold $t$ of the $n$ parties are participating honestly
  - Remaining parties are working together as Eve (passive) or as Mallory (active)
- Then, nothing is revealed about the inputs beyond what can be inferred from the output $y$ (note: this inference problem can be challenging)

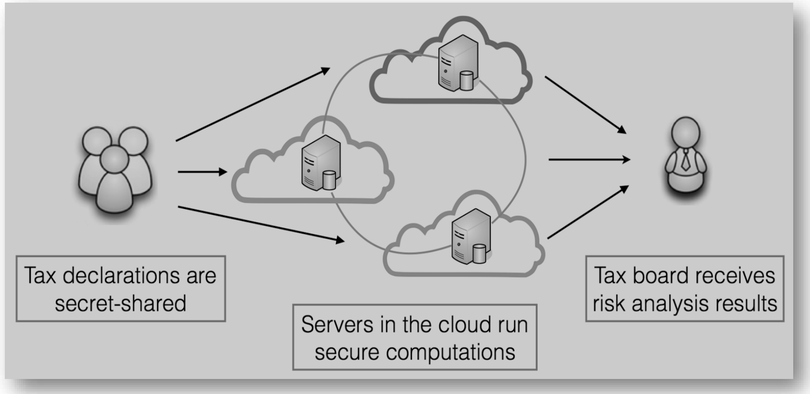
$$y = f(\text{TOP SECRET CONFIDENTIAL TOP SECRET}, \text{TOP SECRET CONFIDENTIAL TOP SECRET}, \text{TOP SECRET CONFIDENTIAL TOP SECRET}, \ldots)$$

# **Cryptography** *enables* **secure data analysis** *for* **social benefit**

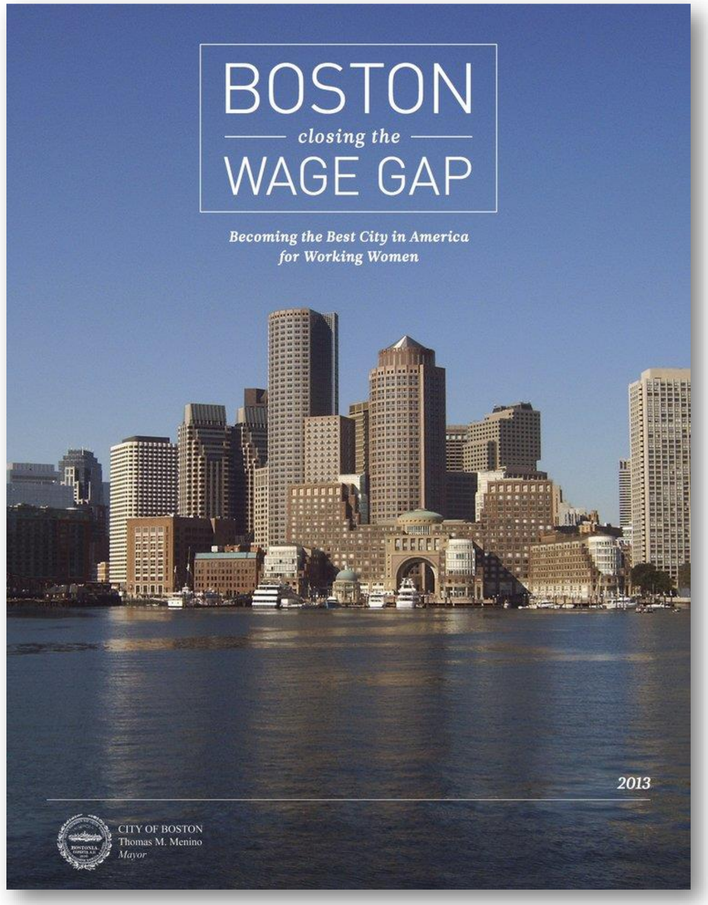
# 2. An example

# Some deployments of MPC in practice

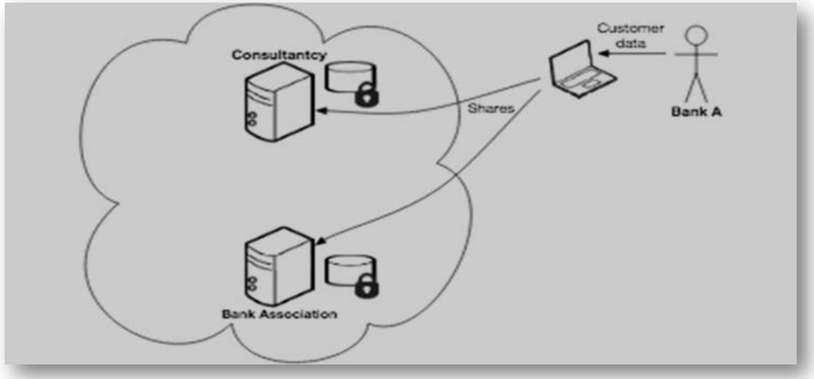
**Cybernetica:** VAT tax audits



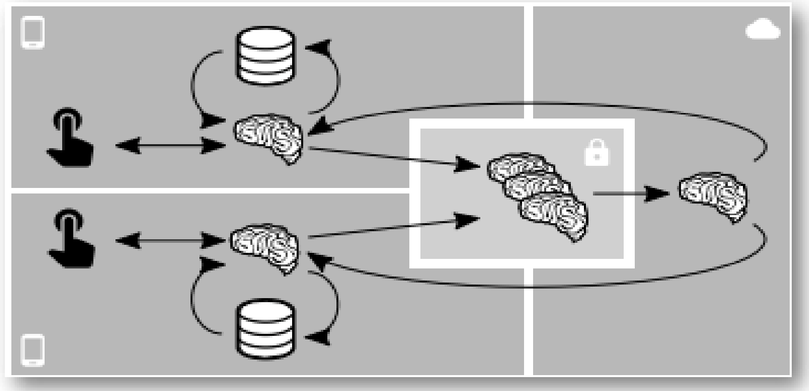

**BU:** Pay equity in Boston



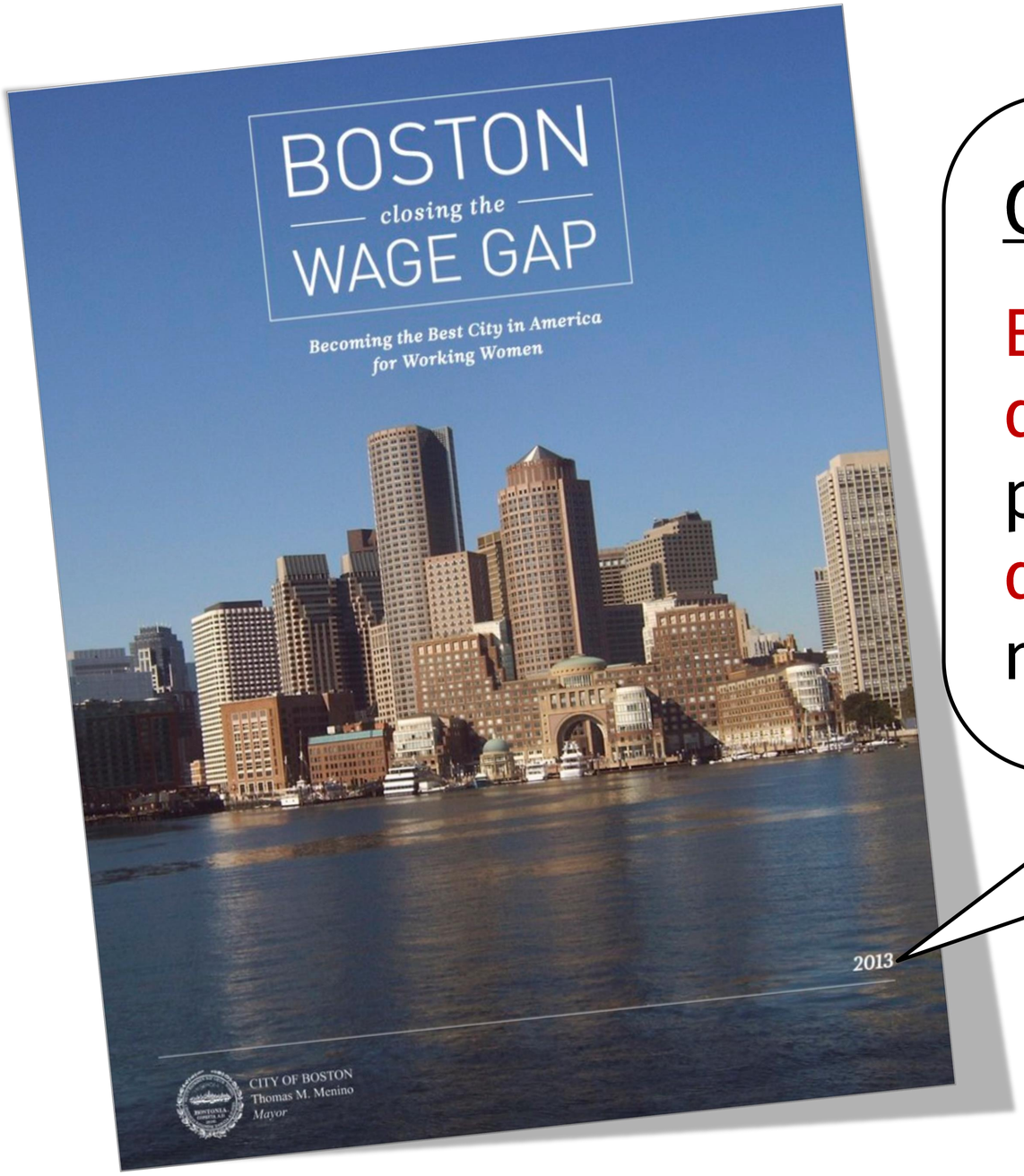

**Partisia:** Rate credit of farmers




**Google:** Federated machine learning



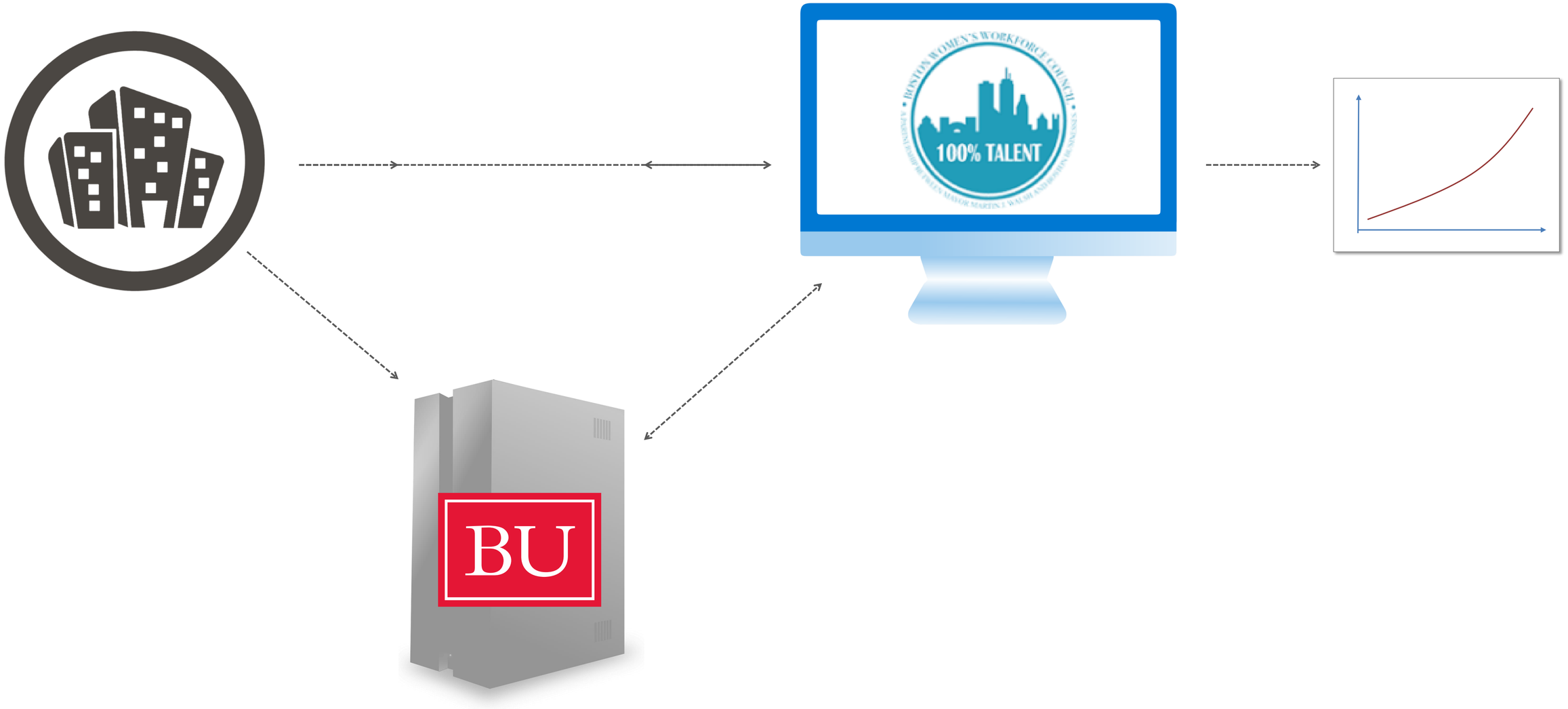
**Unbound:** Protect cryptographic keys




## Goal 3: *Evaluating Success*

Employers agree to … contribute data to a report compiled by a third party on the Compact's success to date. Employer-level data would not be identified in the report.

# Workflow



# Trust spectrum

**Trust us**

**Trust anyone**

BU

BOSTON WOMEN'S WORKFORCE COUNCIL
100% TALENT

**Trust no one**

# How it works


# How it works

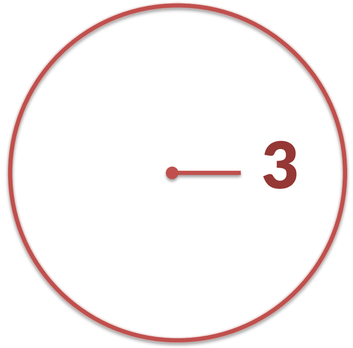

=


+

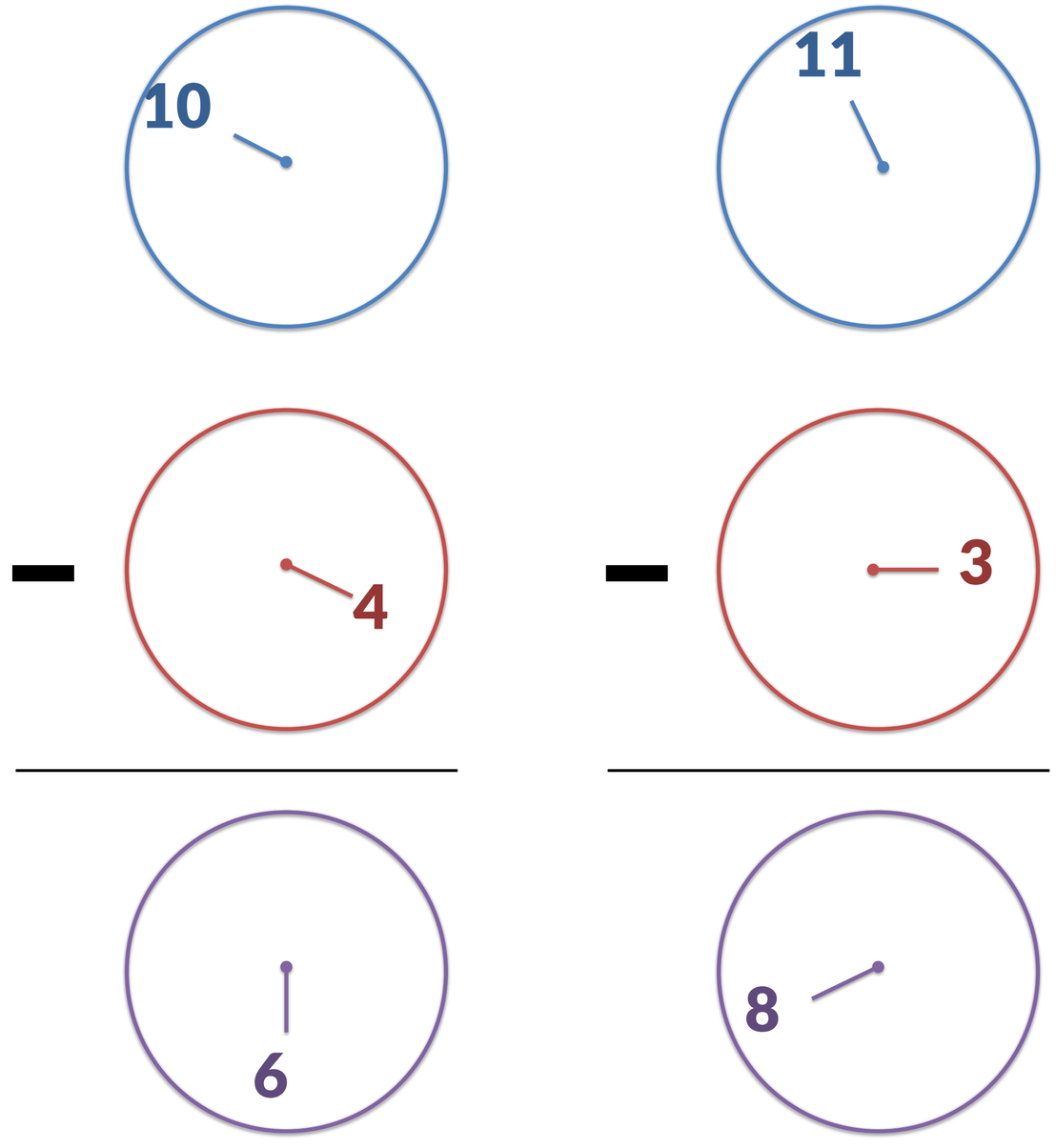


=


+



# How it works



# How it works

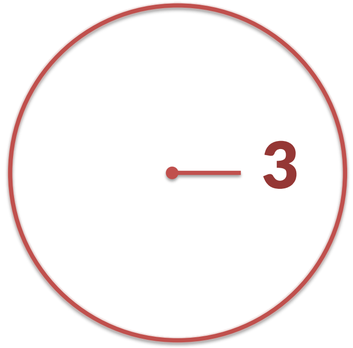

–

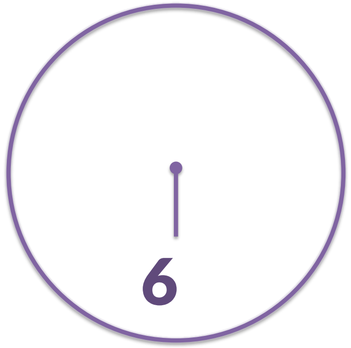


CITY of BOSTON



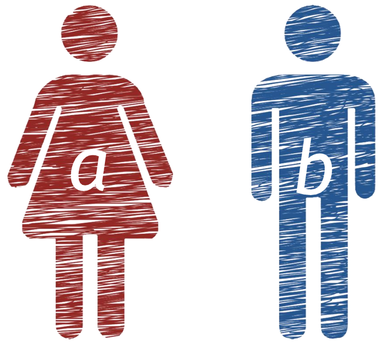

–




# 3. Securely computing linear functions

# Another viewpoint: 3 steps to MPC




Computing servers



$a_1$ $b_1$

$a_2$ $b_2$

Split secrets from data contributors

$y_1 = b_1 - a_1$

$y_2 = b_2 - a_2$

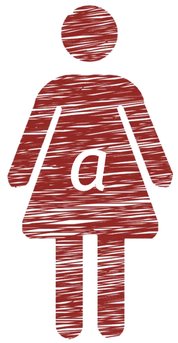
Compute over secret shares

CITY of BOSTON

$y = y_1 + y_2$
$= b - a$

Reconstruct the final answer

# Adding secret + public value




Computing servers



$a_1$ $b$

$a_2$ $b$

$y_1 = a_1 + b$

$y_2 = a_2$

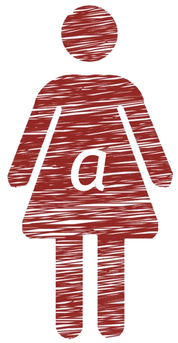
$y = y_1 + y_2$
$= a + b$


Split secrets from data contributors

Compute over secret shares

Reconstruct the final answer

# Scalar multiplication




$a_1$

Computing servers



$a_2$

$y_1 = 2 * a_1$

$y_2 = 2 * a_2$

$y = y_1 + y_2$
$= 2 * a$


Split secrets from data contributors

Compute over secret shares

Reconstruct the final answer

# Simpler notation

Generic server

*Secret share*

$[a]$ $[b]$

*Compute*

$[y] = L([a], [b])$

*Reconstruct*

open $y = L(a, b)$

# Extending to several inputs

Generic server

*Secret share*

$[a]$ $[b]$

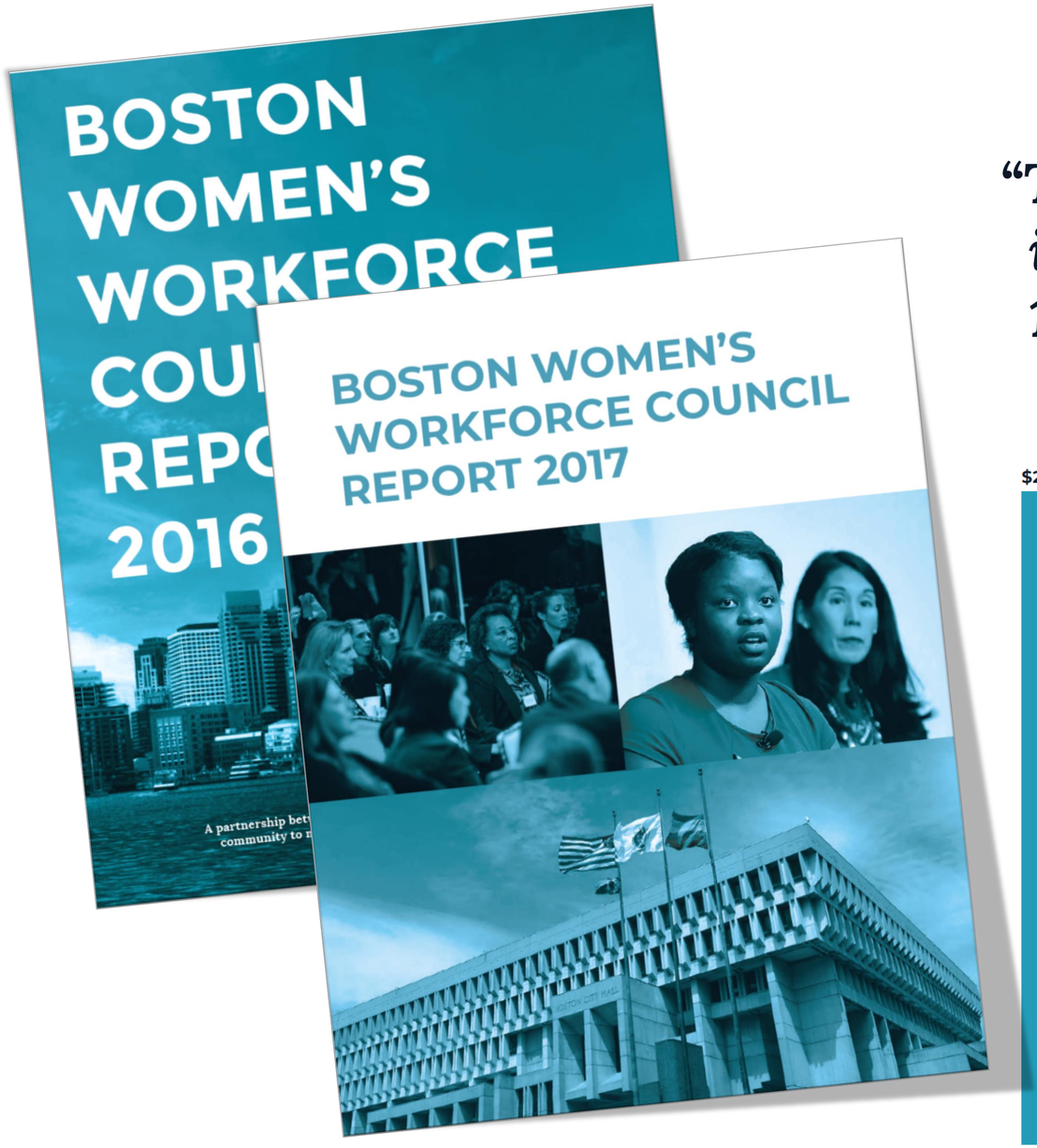
$[c]$ $[d]$

*Compute*

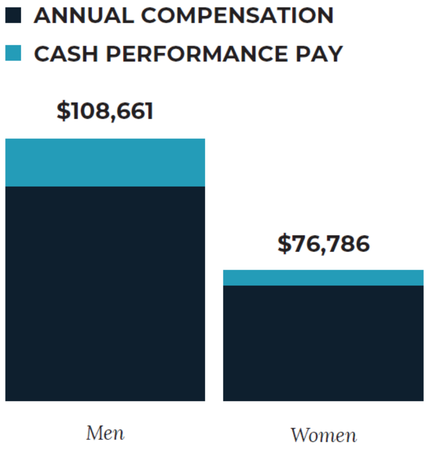
$[y] = [b] + [d] - [a] - [c]$

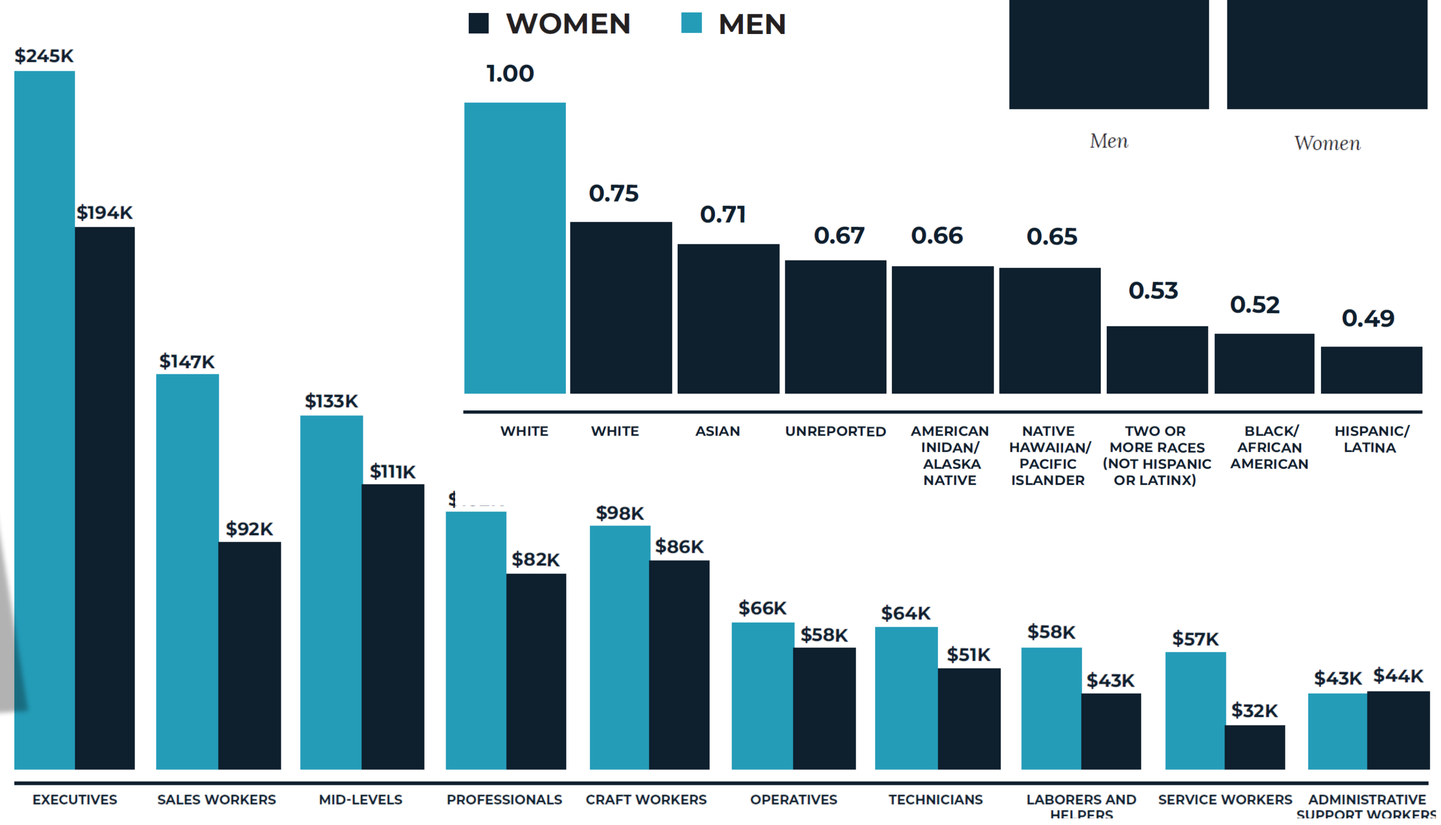
*Reconstruct*

open $y$ from $[y]$




*"This year's data submission included 166,705 employees from 114 Compact-signing companies.*



# Boston Women's Workforce Council

## 100% Talent Data Submission

### Number Of Employees

| | Hispanic or Latinx | | White | | Black/African American | | Native Hawaiian or Pacific Islander | | Asian | | American Indian/Alaska Native | | Two or More Races (Not Hispanic or Latinx) | | Unreported | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | Female | Male | Female | Male | Female | Male | Female | Male | Female | Male | Female | Male | Female | Male | Female | Male |
| Executive/Senior Level Officials and Managers | | | | | | | | | | | | | | | | |
| First/Mid-Level Officials and Managers | | | | | | | | | | | | | | | | |
| Professionals | | | | | | | | | | | | | | | | |
| Technicians | | | | | | | | | | | | | | | | |
| Sales Workers | | | | | | | | | | | | | | | | |
| Administrative Support Workers | | | | | | | | | | | | | | | | |
| Craft Workers | | | | | | | | | | | | | | | | |
| Operatives | | | | | | | | | | | | | | | | |
| Laborers and Helpers | | | | | | | | | | | | | | | | |
| Service Workers | | | | | | | | | | | | | | | | |

# Boston Women's Workforce Council

## 100% Talent Data Submission

### Number Of Employees

| | Hispanic or Latinx | | White | | Black/African American | | Native Hawaiian or Pacific Islander | | Asian | | American Indian/Alaska Native | | Two or More Races (Not Hispanic or Latinx) | | Unreported | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | Female | Male | Female | Male | Female | Male | Female | Male | Female | Male | Female | Male | Female | Male | Female | Male |
| Executive/Senior Level Officials and Managers | | | | | | | | | | | | | | | | |
| First/Mid-Level Officials and Managers | | | | | | | | | | | | | | | | |
| Professionals | | | | | | | | | | | | | | | | |
| Technicians | | | | | | | | | | | | | | | | |
| Sales Workers | | | | | | | | | | | | | | | | |
| Administrative Support Workers | | | | | | | | | | | | | | | | |
| Craft Workers | | | | | | | | | | | | | | | | |
| Operatives | | | | | | | | | | | | | | | | |
| Laborers and Helpers | | | | | | | | | | | | | | | | |
| Service Workers | | | | | | | | | | | | | | | | |

# Gathering Web Analytics using MPC

## Answer additional questions

We have included these questions to get instant feedback as to how this process went in order to improve the process in future years. Please know that the answers to these questions will be anonymous, and they will be considered separately from the encrypted and aggregated data above.

Which department are you in?

- Human Resources (e.g. HR Manager, HRIS Manager, Compensation Manager, Talent & Development)
- Operations (e.g. Director of Operations)
- Diversity (e.g. Chief Diversity Officer)
- Upper Management (e.g. COO, CEO, Executive Director)
- Other

What kind of HRIS or organizational system does your company/organization use?

- Large-scale traditional HRIS/HRMS software (e.g. ADP, Workday, PeopleSoft, etc.)
- Microsoft Office or similar (e.g. Excel, Microsoft Word, Google Docs)
- Other

How easy was it to understand what data was required given the template and instructions?

- Extremely easy
- Moderately easy
- Slightly easy
- Neither easy nor difficult
- Slightly difficult


## Answer additional questions

We have included these questions to get instant feedback as to how this process went in order to improve the process in future years. Please know that the answers to these questions will be anonymous, and they will be considered separately from the encrypted and aggregated data above.

Which department are you in?

- Human Resources (e.g. HR Manager, HRIS Manager, Compensation Manager, Talent & Development)
- Operations (e.g. Director of Operations)
- Diversity (e.g. Chief Diversity Officer)
- Upper Management (e.g. COO, CEO, Executive Director)
- Other

What kind of HRIS or organizational system does your company/organization use?

- Large-scale traditional HRIS/HRMS software (e.g. ADP, Workday, PeopleSoft, etc.)
- Microsoft Office or similar (e.g. Excel, Microsoft Word, Google Docs)
- Other

How easy was it to understand what data was required given the template and instructions?

- Extremely easy
- Moderately easy
- Slightly easy
- Neither easy nor difficult
- Slightly difficult

# 4. Secure multiplication

# Multiplying two secrets

Generic server

*Secret share*

[*w*] [*x*]

*Compute*

[*y*] = ???

*Reconstruct*

*y* = sum([*y*]) = *w* * *x*

# Multiplying two secrets... with help

$$y = (w + a - a) * (x + b - b)$$
$$= (d + a) * (e + b)$$
$$= de + db + ea + c$$

Generic server

*Secret share*

$[w]$ $[x]$

give servers a hint:
random $[a]$, $[b]$, $[c]$
such that $c = a*b$

*Compute*

$[d] = [w] - [a]$
$[e] = [x] - [b]$

$[y] = de + d[b] + e[a] + [c]$

*Reconstruct*

open $d$, $e$

open $y = w * x$

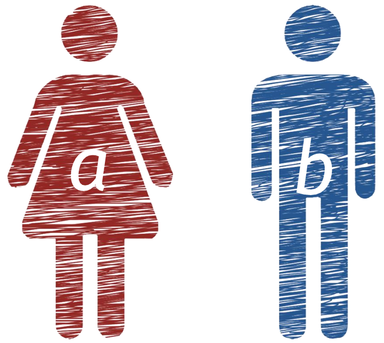
**How do we build this hint?**
**Using (more complicated) MPC!**

# 5. Generic secure computation

# Secure computation of everything

- So far we have seen
  - Secure computing for + and -
  - Secure computing for *
  - Composing multiple secure computations before reconstruction
- + and * form a Turing-complete set of gates
- Ergo, we can compose them to do secure computation of any function *f*
  - (This may not be the *fastest* way to compute *f* securely, however…)

# Secure Boolean XOR: a new way of splitting secrets!




Computing servers



$a_1$ $b_1$

$a_2$ $b_2$

Split secrets s.t.
$a = a_1 \oplus a_2$

$y_1 = a_1 \oplus b_1$

$y_2 = a_2 \oplus b_2$

Compute over secret shares


$y = y_1 \oplus y_2$
$= a \oplus b$

Reconstruct the final answer

# Secure Boolean AND... with help

$$y = (w \oplus a \oplus a) \wedge (x \oplus b \oplus b)$$
$$= (d \oplus a) \wedge (e \oplus b)$$
$$= de \oplus db \oplus ea \oplus c$$

Generic server

*Secret share*

$\langle w \rangle$ $\langle x \rangle$

give servers a hint:
random $\langle a \rangle, \langle b \rangle, \langle c \rangle$
such that $c = a \wedge b$

*Compute*

$\langle d \rangle = \langle w \rangle \oplus \langle a \rangle$
$\langle e \rangle = \langle x \rangle \oplus \langle b \rangle$

$\langle y \rangle = de \oplus d\langle b \rangle \oplus e\langle a \rangle \oplus \langle c \rangle$

*Reconstruct*

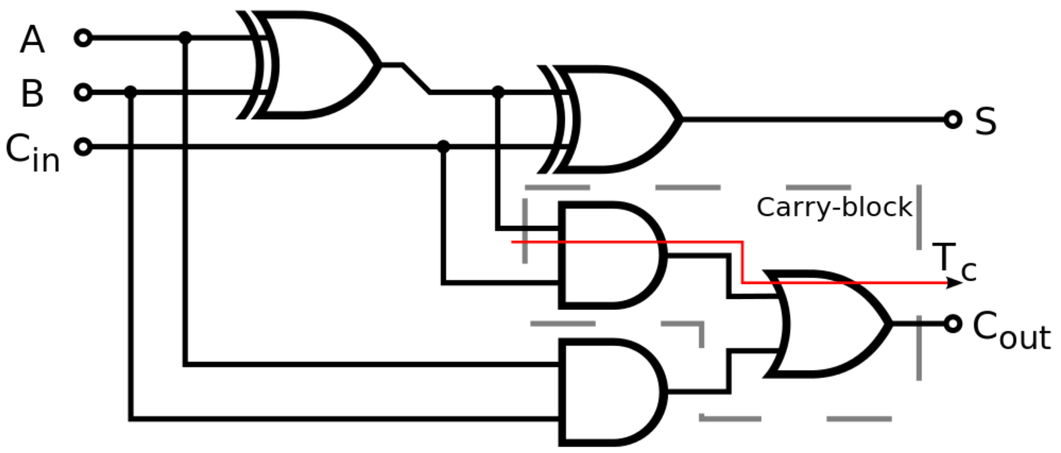
open $d$, $e$

open $y = w \wedge x$

**How do we build this hint?**
**Using (more complicated) MPC!**

# Converting between arithmetic and boolean

- Problem
  - Servers have additive sharing $[x]$ of a secret $x = x_1 + x_2 + \ldots + x_n$
  - Want a Boolean sharing $\langle x \rangle$
- Solution
  - Each party builds a Boolean sharing of its own share $\langle x_i \rangle$
  - Securely compute the Boolean circuit that does ripple-carry addition of $x_i$
  - Result: Boolean sharing of the sum $x$!




Source: https://en.wikipedia.org/wiki/Adder_(electronics)

# Benefit of cryptographically secure computation

- MPC says nothing about which data analyses are worthwhile to compute
- MPC de-couples discussion of *what* to compute from *how* to do so
- MPC expands the Pareto frontier of possible data analyses