DEPLOYING MPC FOR SOCIAL GOOD

Lucy Qin
Research Software Engineer | Software & Application Innovation Lab | Boston University

Andrei Lapets, Frederick Jansen, Kinan Bab, Peter Flockhart, Rawane Issa, Mayank Varia, Azer Bestavros
MPC FOR SOCIAL GOOD

Hey, Charlie
Combatting Opioid Addiction

BWWC
BOSTON WOMEN'S WORKFORCE COUNCIL
Pay Equity

Medical Data Sharing

Greater Boston Chamber of Commerce
Economic Inclusion

The Dataverse Project
Social Science Research Sharing

CALLISTO
Detecting Serial Perpetrators of Sexual Misconduct
MPC FOR SOCIAL GOOD

Hey, Charlie
Combatting Opioid Addiction

Greater Boston Chamber of Commerce
Economic Inclusion

BWWC
Pay Equity

The Dataverse Project
Social Science Research Sharing

CALLISTO
Detecting Serial Perpetrators of Sexual Misconduct

Medical Data Sharing
SECURE MULTI-PARTY COMPUTATION (MPC)

\[ f(s_1, s_2, s_3) = z \]

private inputs

public output
CLOSING THE WAGE GAP IN BOSTON

1. Understanding the root causes of the wage gap
2. Closing the gap
3. Evaluating success

Over 200 Businesses
ORIGINALLY PROPOSED WORKFLOW

Business A

Salary Data

Trusted 3rd Party

Salary Data

Business B

Results!
ROLES & CONCERNS

- Lawyer
- BWWC
- HR/Diversity Personnel
- IT Personnel
ROLES & CONCERNS

Lawyer
Liability

BWWC

HR/Diversity Personnel

IT Personnel
ROLES & CONCERNS

Lawyer
Liability

BWWC
Participation

HR/Diversity Personnel

IT Personnel
ROLES & CONCERNS

Lawyer
Liability

BWWC
Participation

HR/Diversity
Personnel
Usability

IT Personnel
ROLES & CONCERNS

Lawyer
Liability

BWWC
Participation

HR/Diversity
Personnel
Usability

IT Personnel
Auditability
**MPC SOLUTION**

**Contributor A**
- actual data $A$ + random mask $A$ = masked data $A$

**Contributor B**
- actual data $B$ + random mask $B$ = masked data $B$

**BU Server (web server/database)**
- masked data $A$ + masked data $B$ = masked aggregate data

**Analyst at BWWC (client running web browser)**
- masked aggregate data

**Public-key Encrypted Storage**
- Analyst never accesses the data
- only Analyst has key;
  no one else (including BU) can read the content of this data

**Masked Aggregate Data**
- random mask $A$ + random mask $B$ = aggregate mask
- aggregate mask + actual aggregate data = actual aggregate data
Please make sure your session key and participation code match the ones provided in the email sent to you by the BWWC. Drag and drop your completed template file to encrypt and include your submission in the aggregate data.

### Total Annual Compensation (Dollars)

<table>
<thead>
<tr>
<th></th>
<th>Hispanic or Latinx</th>
<th>White</th>
<th>Black/African American</th>
<th>Native Hawaiian or Pacific Islander</th>
<th>Asian</th>
<th>American Indian/Alaska Native</th>
<th>Two or More Races (Not Hispanic or Latinx)</th>
<th>Unreported</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Female</td>
<td>Male</td>
<td>Female</td>
<td>Male</td>
<td>Female</td>
<td>Male</td>
<td>Female</td>
<td>Male</td>
</tr>
</tbody>
</table>

- 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

**Submit**
ERROR CHECKING

Verify and submit your data
Please ensure that all data entered is accurate, and confirm that all employees are accounted for by reviewing the total number of employees below.

Totals Check

<table>
<thead>
<tr>
<th></th>
<th>Total Number of Employees</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Female</td>
</tr>
<tr>
<td>Total</td>
<td>15905</td>
</tr>
</tbody>
</table>

Errors

- Invalid session number
- Invalid participation code
- Please answer all Additional Questions

Submission history

- You have not submitted yet

Submit
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
USER EXPERIENCE & WEB ANALYTICS

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
“In 2014, we had 38 companies committed to the 100% Talent Compact. Today, that number is over 250. That’s a huge percentage of our workforce committing to include their wage data in our analysis and promote and retain more women.”

Mayor Martin J. Walsh,
4th Annual Effective Practices Conference
LATINA WOMEN IN GREATER BOSTON EARN JUST $0.49 FOR EVERY DOLLAR WHITE MEN MAKE

THE BOSTON WOMEN’S WORKFORCE COUNCIL IS COMMITTED TO GENDER EQUITY FOR ALL WOMEN. VISIT OUR WEBSITE AND SIGN THE 100% TALENT COMPACT TODAY.

WWW.BOSTONWOMENSWORKFORCECOUNCIL.COM
#100PERCENTTALENT #EQUALPAYBOS

FIGURE 8: Average compensation by EEO-1 Job Category

- WOMEN
- MEN

- EXECUTIVES: $245K
- SALES WORKERS: $194K
- MID-LEVELS: $147K
- PROFESSIONALS: $133K
- CRAFT WORKERS: $111K
- OPERATIVES: $102K
- TECHNICIANS: $82K
- LABORERS AND HELPERS: $86K
- SERVICE WORKERS: $66K
- ADMINISTRATIVE SUPPORT WORKERS: $58K
- $57K
- $43K
- $32K
- $43K
- $44K
FROM DATA TO IMPACT

UPCOMING EVENTS

Thank you for making 2017 a success! We hope to see you at our upcoming events in 2018/19.

Q4 BRIEFING: WOMEN’S LEADERSHIP ORGANIZATIONS - ACADEMICS AND ACTIVISTS

DATE: October 24, 2018
TIME: 7:30-9:30 AM

ANNUAL BEST PRACTICES CONFERENCE

DATE: December 4, 2018
TIME: 8:00-10:30 AM

Q1 BRIEFING: TECHNOLOGY GAME CHANGERS

DATE: January 31, 2019
TIME: 7:30-9:30 AM

SAVE THE DATE

LOCATIONS TBD

Sign up for our newsletter on our website bostonwomensworkforcecouncil.com for updates!
SUPPORTING LOCAL MINORITY-OWNED BUSINESSES

Pacesetters
Data Submission

Input your data
Please make sure your session key and participation code match the ones provided in the email sent to you by the Greater Boston Chamber of Commerce. Drag and drop your completed template file to encrypt and include your submission in the aggregate data.

Session key

Participation code

Drag and drop your completed template file here

Choose file

View your data
Your data will appear here after you drag/drop or browse to find your completed Excel template file above.

Entered Data
Any red cells indicate an error - click on the cell to see the error message.
Yellow cells indicate the value might be outside of the expected range. Please double-check to make sure the data is correct. You will still be able to submit your data.
For a list of definitions, please click here.

Amount spent with MBEs

<table>
<thead>
<tr>
<th></th>
<th>Value for FY17 in Thousands of Dollars</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dollar Amount Spent with Local MBEs</td>
<td>$345K</td>
</tr>
<tr>
<td>Dollar Amount Spent with State MBEs</td>
<td>$33K</td>
</tr>
<tr>
<td>Dollar Amount Spent with National MBEs</td>
<td>$200K</td>
</tr>
</tbody>
</table>
DETECTING SERIAL PERPETRATORS OF SEXUAL MISCONDUCT

6x more likely to report through a school’s Callisto website than to their school or the police

3x more likely to seek out medical and emotional support services after using Callisto

15% of survivors were matched with another survivor who reported the same perpetrator
Identifying information about a **survivor** and the **accused** can only be decrypted by a lawyer when **at least 2 users** name the same perpetrator.

---

**Callisto: A Cryptographic Approach To Detect Serial Predators Of Sexual Misconduct**

Anjana Rajan  Lucy Qin  David Archer
Dan Boneh  Tancrède Lepoint  Mayank Varia

March 29, 2018
Last updated: November 14, 2018

**Abstract**

Callisto, a non-profit that has created an online sexual assault reporting platform for college campuses, has expanded its work to combat sexual assault and professional sexual coercion in other industries. In our new product, users will be invited to an online matching escrow that will detect repeat perpetrators and create pathways to support for victims. Users of this product enter incident details and perpetrator identities into the escrow. This data can only be decrypted by a Legal Options Counselor (a third-party lawyer vetted by Callisto) when at least one other user enters the identity of the same perpetrator. If perpetrator identities match, each user is assigned a Legal Options Counselor, who will connect users to each other (if appropriate) and help each user determine their best path towards justice. User relationships with Legal Options Counselors are structured so that relevant communications benefit from client-counselor privilege. A combination of client-side encryption, encrypted communication channels, oblivious pseudo-random functions, key federation, and Shamir Secret Sharing keep data encrypted so that only Legal Options Counselors gain access to identifying user submitted data when a perpetrator match is identified. In this paper, we present an informal risk management assessment, threat model, and cryptographic solution overview for our new product. A later paper will provide a formal security analysis and mathematical proofs of our cryptographic scheme.
DETECTING SERIAL PERPETRATORS OF SEXUAL MISCONDUCT

Alice → Accused: Mallory → Alice Mallory
Bob → Accused: Mallory → Bob Mallory
Carlos → Accused: Eve → Carlos Eve
where \((x, y)\) is a share

\[
y = ax + k
\]

hashed user id

key represented as y-intercept

share

value \((y)\)

hashed user id \((x)\)
1. Welcome. We believe you.

Before you begin, please know that you are not alone. We have created this guide to share information and resources for survivors of sexual assault, rape, and sexual coercion. We hope that you find it helpful.

We know that this time in your life can be very stressful and that much of the language here may be triggering or upsetting. However, we also hope that you find this guide to be empowering and uplifting. It is written by fellow survivors to remind you that you are surrounded by a community of caring individuals, and that there are many resources available to help you on your journey.

Our encryption method focuses on several cryptography techniques (our white paper explains these in more detail.) This demo highlights two techniques: client side encryption and Shamir Secret Sharing.

To begin, enter a user name and perpetrator name. This data will be encrypted with a record key, $k_i$. Data inputs will not be stored.
DEPLOYING MPC FOR SOCIAL GOOD
THANK YOU

multiparty.org
sail.bu.edu

/multiparty
/hicsail

@lcyqn
@bu_computing
@hicsail