FROM USABILITY TO SECURE COMPUTING AND BACK AGAIN

Lucy Qin, Andrei Lapets, Frederick Jansen, Peter Flockhart, Kinan Dak Albab, Ira Globus-Harris, Shannon Roberts*, Mayank Varia

Boston University
*University of Massachusetts Amherst

Symposium on Usable Privacy and Security (SOUPS) 2019
BOSTON closing the WAGE GAP

Becoming the Best City in America for Working Women

In 2016, women in Boston earned:

76 cents for every man's dollar*
ORIGINALLY PROPOSED WORKFLOW

Business A

Salary Data

Business B

Salary Data

Trusted 3rd Party

Results!
ORIGINALLY PROPOSED WORKFLOW
computing without directly sharing data: secure multi-party computation (MPC)

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

private inputs

public output
COMPUTING WITHOUT DIRECTLY SHARING DATA: SECURE MULTI-PARTY COMPUTATION (MPC)

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

private inputs

public output
### 2016 vs 2017

<table>
<thead>
<tr>
<th>Category</th>
<th>2016</th>
<th>2017</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total # of employers</td>
<td>69</td>
<td>114</td>
</tr>
<tr>
<td># employees (1000s)</td>
<td>113</td>
<td>167</td>
</tr>
<tr>
<td>% of workforce</td>
<td>11</td>
<td>16</td>
</tr>
<tr>
<td>Total annual earnings</td>
<td>$11b</td>
<td>$15b</td>
</tr>
</tbody>
</table>
USABILITY

SECURE MULTI-PARTY COMPUTATION
USABILITY CHALLENGES

1.) INSPIRING TRUST
2.) ERROR MINIMIZATION
3.) EASE OF USE
1. The analyst initiates the process by generating a secret and public RSA key pair \((x, p)\) and a unique session identifier \(id\). Submitting \(p\) to the service provider, and sending \(id\) to all the contributors.

2. Each of the \(n\) contributors possesses a secret data value \(d_i \in G\) and does the following at least once:
   (a) Generate a secret random mask \(m_i \in G\) and calculate the masked
   (b) Receive \(p\) from
   (c) Send \(r_i\) and \(c_i\) -

3. The service provider computes the sum of the masked data values to obtain the aggregate masked data quantity \(R = \sum_{i=1}^{n} r_i\).

4. The analyst then retrieves \(R\) and all the \(c_1, \ldots, c_n\) from the service provider, computes \(m_i = \text{Dec}(c_i)\) for all \(i\), computes \(M = \sum_{i=1}^{n} m_i\), and obtains the final result \(R = M - \sum_{i=1}^{n} d_i\). No other party receives any output.

**cryptographic proofs**

**concrete analogies**
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

random mask A + random mask B = aggregate mask

random aggregate data
Contributor A

BU Server
(web server/database)

Contributor B

Analyst at BWWC
(client running web browser)
Contributor A

actual data A + random mask A

Contributor B

actual data B + random mask B

BU Server
(web server/database)

Analyst at BWWC
(client running web browser)
Contributor A

actual data A + random mask A

Contributor B

actual data B + random mask B

BU Server (web server/database)

random mask A
random mask B
random mask A
random mask B

Analyst at BWWC (client running web browser)

random mask A + random mask B = aggregate mask
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)

Analyst at BWWC (client running web browser)

random mask A + random mask B = aggregate mask
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)

random mask A + random mask B = aggregate mask

masked aggregate data

random mask A

random mask B
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)

random mask A + random mask B = aggregate mask

masked aggregate data - aggregate mask = actual aggregate data
ERROR MINIMIZATION

• Since inputs are private, it is difficult to detect and correct invalid data
ERROR MINIMIZATION

- Since inputs are private, it is difficult to detect and correct invalid data
- Error detection logic run under MPC increases overhead
ERROR MINIMIZATION

- Since inputs are private, it is difficult to detect and correct invalid data
- Error detection logic run under MPC increases overhead
- Inherent tradeoff between participation rate and correctness
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
EASE OF USE

Boston Women's Workforce Council
100% Talent Data Submission

Input your data

Please make sure your BWWC 2019 Submission ID and participation code match the ones provided in the email sent to you by the Boston Women's Workforce Council. Drag and drop your completed template file to encrypt and include your submission in the aggregate data.

**BWWC 2019 Submission ID**

![Checkmark icon] dn51w20bdfwfbw5ycvsdr4763w

**Participation code**

![Checkmark icon] bteq93cktxenwmjbssdwh05gr

Drag and drop your completed template file here

—or—

Choose file
USABILITY

SECURE MULTI-PARTY COMPUTATION
USABILITY

SECURE MULTI-PARTY COMPUTATION
WEB ANALYTICS

A

CONTROL

B

VARIATION

23%

37%
WEB ANALYTICS

Activity Feed

TODAY, JUNE 5, 2018

9:42 AM  Purchase Song
9:42 AM  Play Song
9:42 AM  Log In
9:41 AM  Home Page Viewed

Gender

Events performed by the user

images from Mixpanel and Google Analytics
WEB ANALYTICS

images from Mixpanel and Google Analytics
WEB ANALYTICS
REPURPOSING WHAT WE’VE BUILT: MPC

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

Usability Metrics

Aggregate Usability Metrics
USABILITY METRICS UNDER MPC

Browser

Time Spent

UI Feature

Errors
# Version 1

## Enter Session Key

!3k3qphb39xig6d89

## Enter Participation Code

$nhdr28x60xk2bb447

### Amount Spent with MBEs

<table>
<thead>
<tr>
<th></th>
<th>Value for FY in Thousands of Dollars ($)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dollar Amount Spent with Local MBEs ($)</td>
<td>$11K</td>
</tr>
<tr>
<td>Dollar Amount Spent with State MBEs ($)</td>
<td>$52K</td>
</tr>
<tr>
<td>Dollar Amount Spent with National MBEs ($)</td>
<td>$23,000,000K</td>
</tr>
</tbody>
</table>

### Addressable Spend

<table>
<thead>
<tr>
<th></th>
<th>Value for FY18 in Thousands of Dollars</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total Dollar Amount Spent Procuring All Goods and Services Locally ($)</td>
<td></td>
</tr>
<tr>
<td>Total Dollar Amount Spent Procuring All Goods and Services at the State Level ($)</td>
<td>$39K</td>
</tr>
<tr>
<td>Total Dollar Amount Spent Procuring All Goods and Services in the United States ($)</td>
<td>$521K</td>
</tr>
</tbody>
</table>

### Number of MBEs

<table>
<thead>
<tr>
<th>Number of MBEs With Whom You Have Done Business ($)</th>
<th>Value for FY18</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number of Local MBEs With Whom You Have Done Business ($)</td>
<td>12</td>
</tr>
<tr>
<td>Number of State MBEs With Whom You Have Done Business ($)</td>
<td>56</td>
</tr>
<tr>
<td>Number of National MBEs With Whom You Have Done Business ($)</td>
<td>199</td>
</tr>
</tbody>
</table>

All numbers are verified and correct.
**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](#).

<table>
<thead>
<tr>
<th>Amount Spent with MBEs</th>
<th>Value for FY18 in Thousands of Dollars</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dollar Amount Spent with Local MBEs</td>
<td>$10,000K</td>
</tr>
<tr>
<td>Dollar Amount Spent with State MBEs</td>
<td>$923K</td>
</tr>
<tr>
<td>Dollar Amount Spent with National MBEs</td>
<td>$657K</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Addressable Spend</th>
<th>Value for FY18 in Thousands of Dollars</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total Dollar Amount Spent Procuring All Goods and Services Locally</td>
<td>$134,000K</td>
</tr>
<tr>
<td>Total Dollar Amount Spent Procuring All Goods and Services at the State Level</td>
<td>$134,000K</td>
</tr>
<tr>
<td>Total Dollar Amount Spent Procuring All Goods and Services in the United States</td>
<td>$134,000K</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Number of MBEs</th>
<th>Value for FY18</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number of Local MBEs With Whom You Have Done Business</td>
<td></td>
</tr>
<tr>
<td>Number of State MBEs With Whom You Have Done Business</td>
<td></td>
</tr>
<tr>
<td>Number of National MBEs With Whom You Have Done Business</td>
<td></td>
</tr>
</tbody>
</table>
Input your 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.

Session key

Participation code

Drag and drop your completed template file here

—or—

Choose file
RESULTS FROM USABILITY STUDY

Number of Errors by Type and Application Version

- **Empty Cell**
- **Invalid Cell**
- **Submission Cell**
- **No Confirmation**
- **Total**

- **Version 1**
- **Version 2**
- **Version 3**

# of Errors
RESULTS FROM USABILITY STUDY

Time Spent by Application Version

- **Version 1**
  - Session Area: 100 seconds
  - Data Entry: 130 seconds
  - Submit Area: 10 seconds

- **Version 2**
  - Session Area: 150 seconds
  - Data Entry: 250 seconds
  - Submit Area: 0 seconds

- **Version 3**
  - Session Area: 120 seconds
  - Data Entry: 300 seconds
  - Submit Area: 0 seconds

Time (seconds)
LIMITATIONS

limited statistics

configuration must suit MPC
LESSONS LEARNED

1. Error checking, resubmission minimize the chance that errors propagate to final output

2. It’s possible to adapt standard techniques to improve usability even in privacy-preserving contexts
USABILITY

SECURE MULTI-PARTY COMPUTATION
THANK YOU

Azer Bestavros, Rose Kelly, Nina Taft

lucyq@brown.edu
pflock@bu.edu
/multiparty/web-mpc
/multiparty/jiff
multiparty.org
MPC WORKFLOW

Business A

Salary Data

Mask

Masked Data

Business B

BBWC

+ =

Masked Data