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

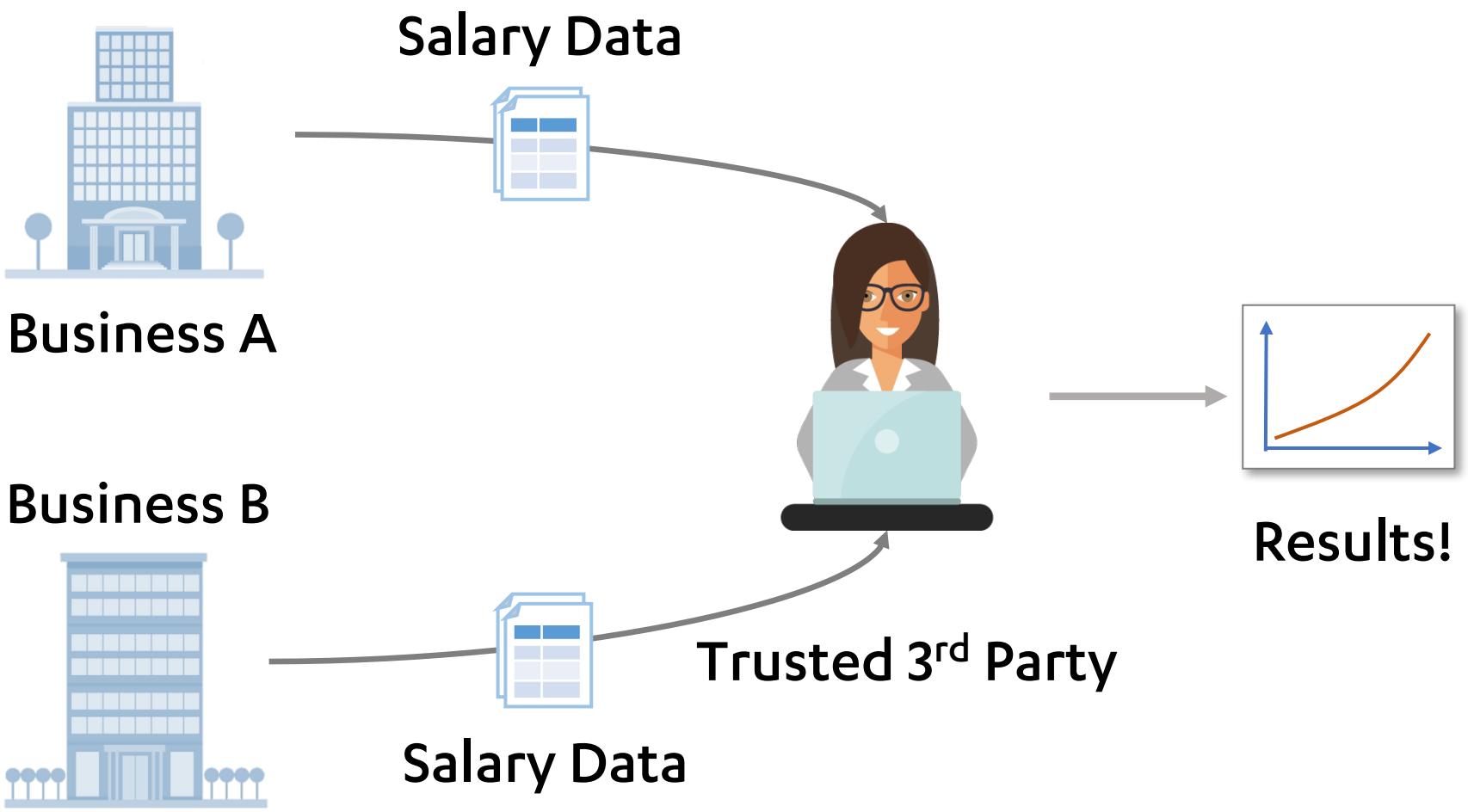
BOSTON
closing the
WAGE GAP

Becoming the Best City in America for Working Women

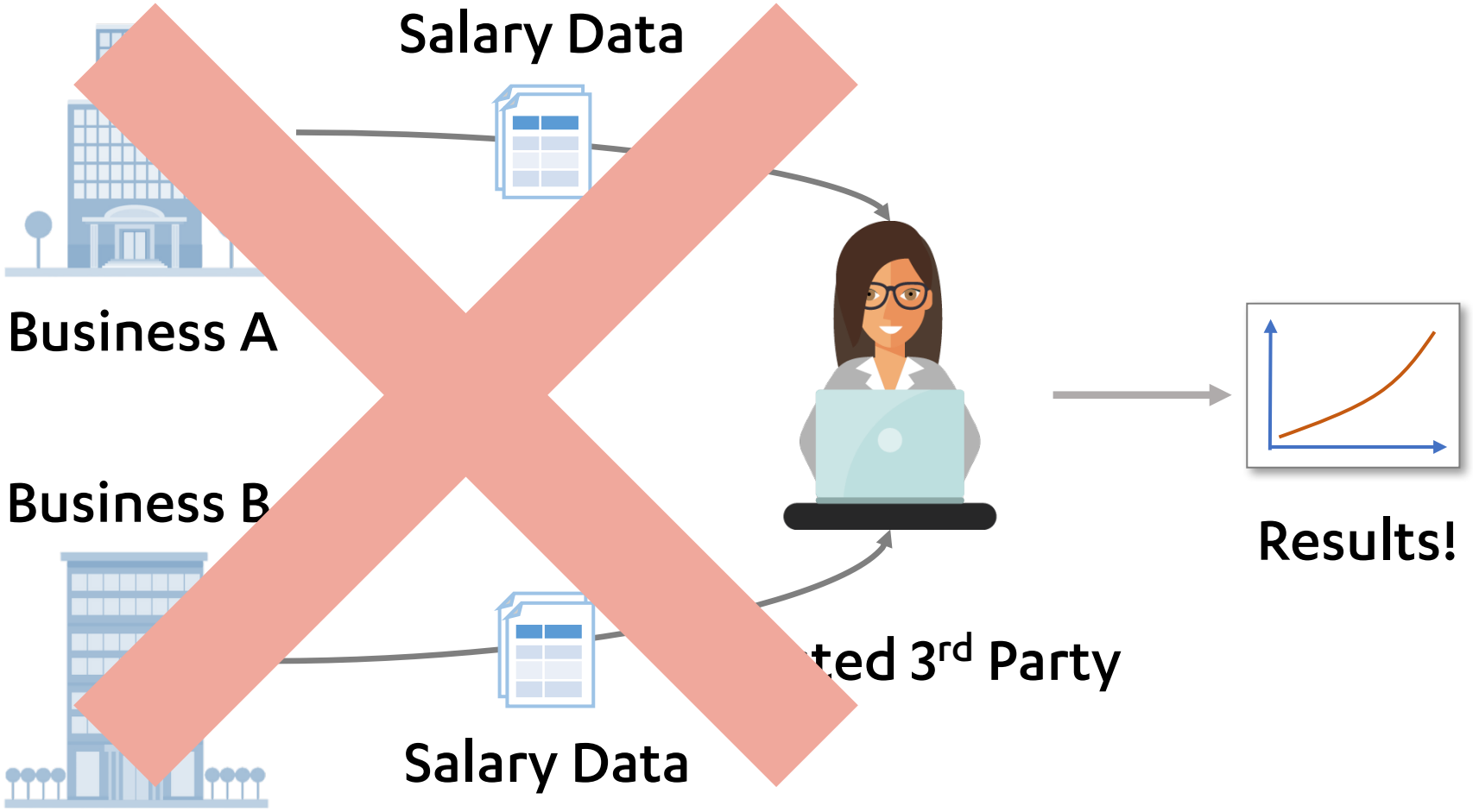
BWWC

BOSTON WOMEN'S WORKFORCE COUNCIL

ORIGINALLY PROPOSED WORKFLOW



ORIGINALLY PROPOSED WORKFLOW



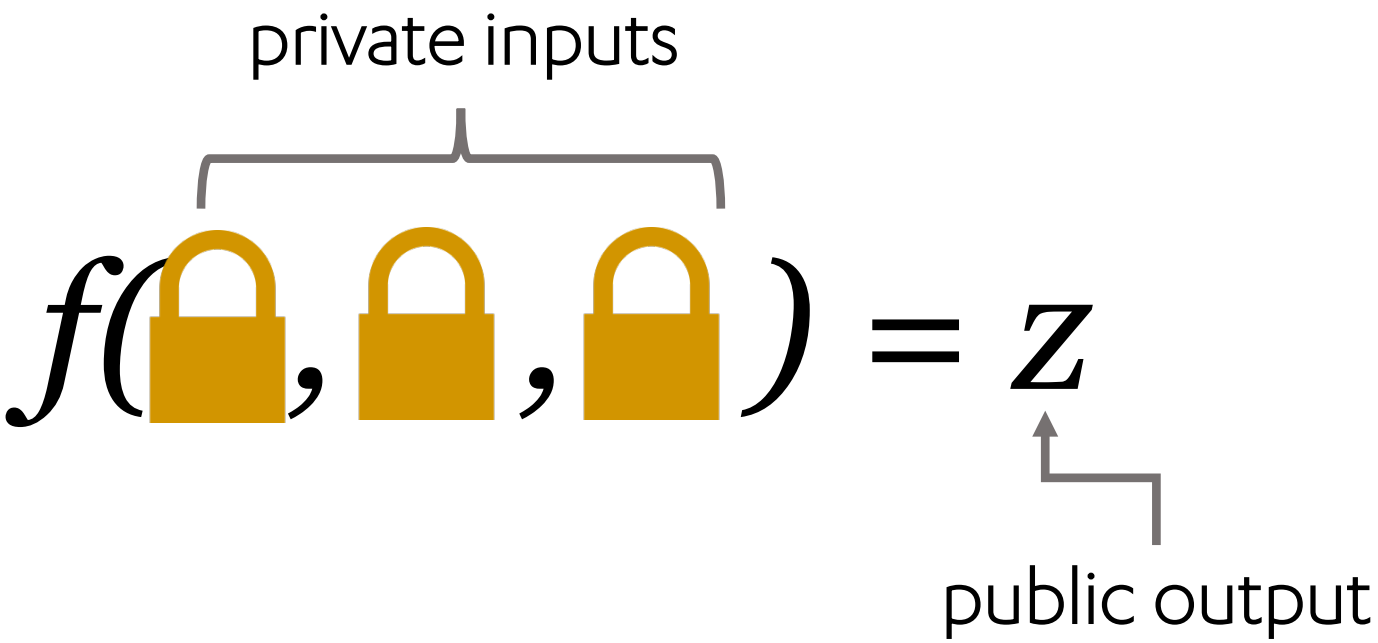
COMPUTING WITHOUT DIRECTLY SHARING DATA: SECURE MULTI-PARTY COMPUTATION (MPC)

private inputs

$$f(s_1, s_2, s_3) = z$$

public output

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



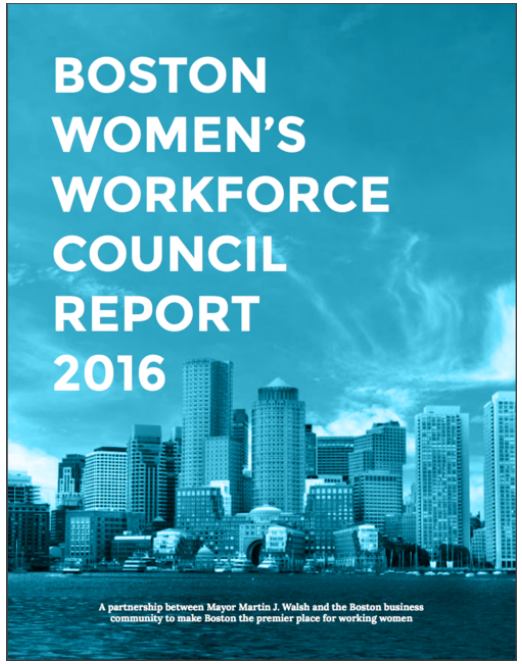
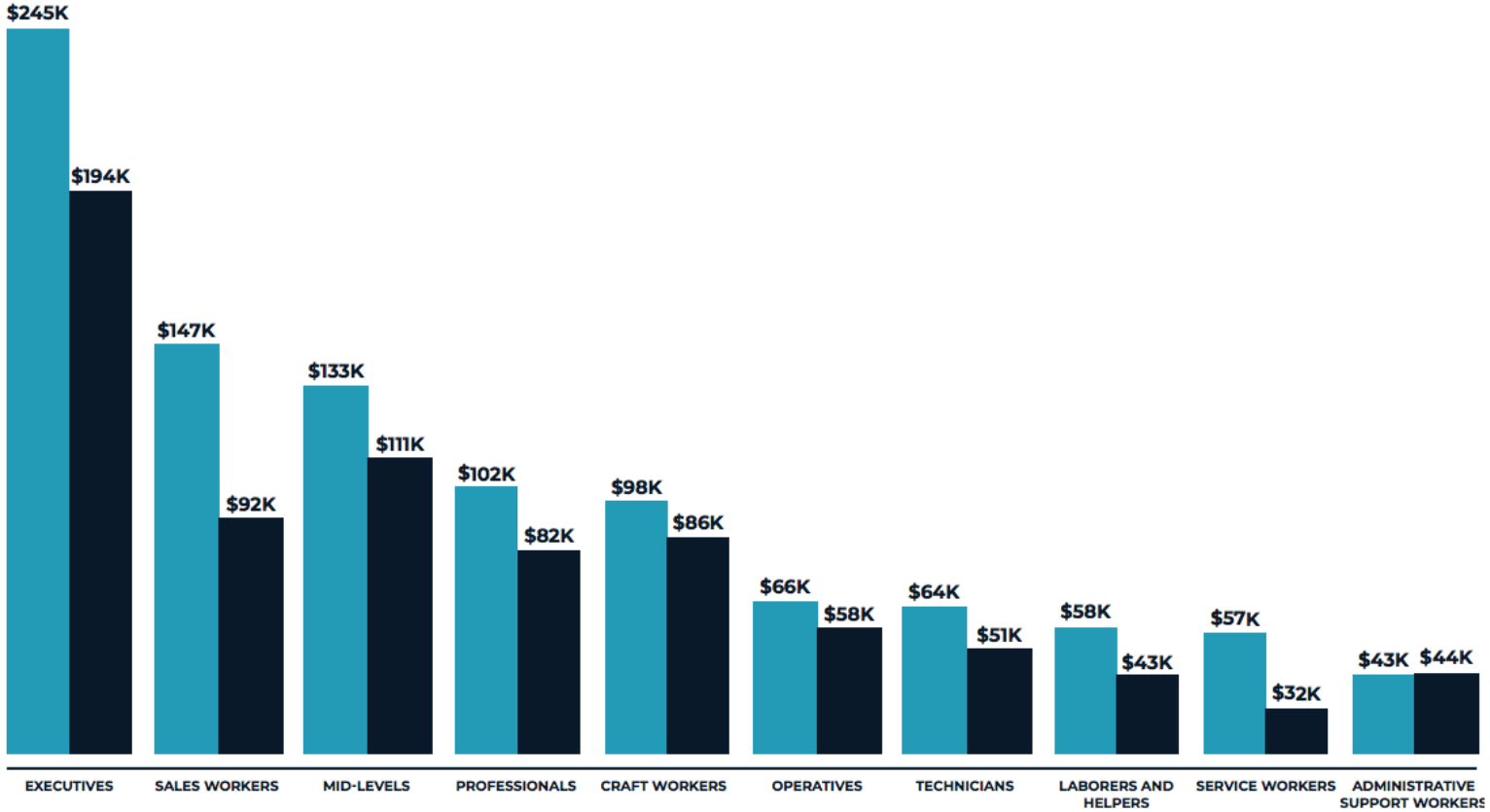
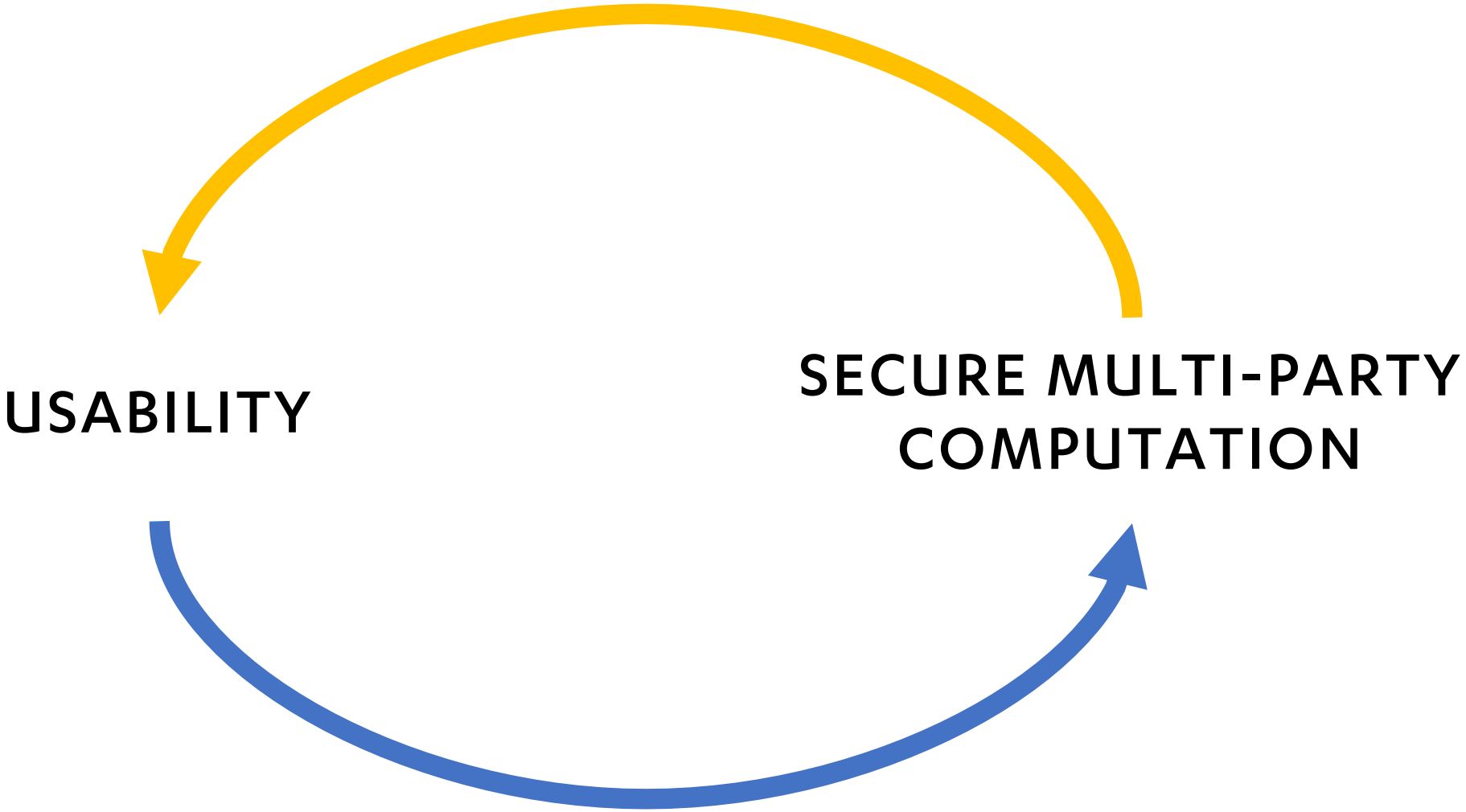
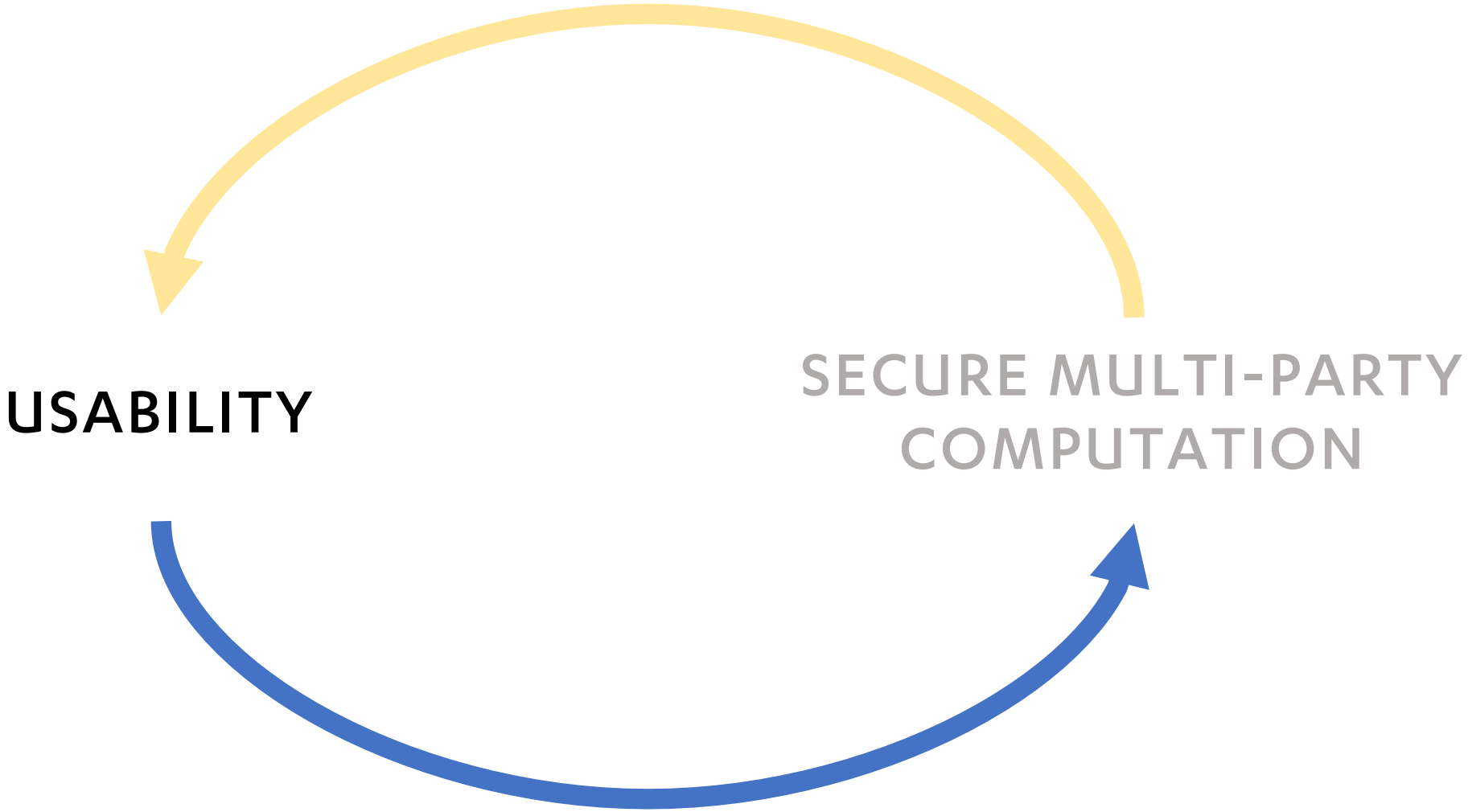


FIGURE 8: *Average compensation by EEO-1 Job Category*



	2016	2017
total # of employers	69	114
# employees (1000s)	113	167
% of workforce	11	16
total annual earnings	$11b	$15b


USABILITY
SECURE MULTI-PARTY COMPUTATION


USABILITY
SECURE MULTI-PARTY COMPUTATION

USABILITY CHALLENGES

1.) INSPIRING TRUST
2.) ERROR MINIMIZATION
3.) EASE OF USE

INSPIRING TRUST

1. The analyst initiates the process by generating a secret and public RSA key pair (s, p) and a unique session identifier $\mathrm{id} \in \mathbb{N}$, submitting p to the service provider, and sending id to all the contributors;[4]

2. Each of the n contributors possesses a secret *data* value $d_i \in G$ and does the following at least once[5]:

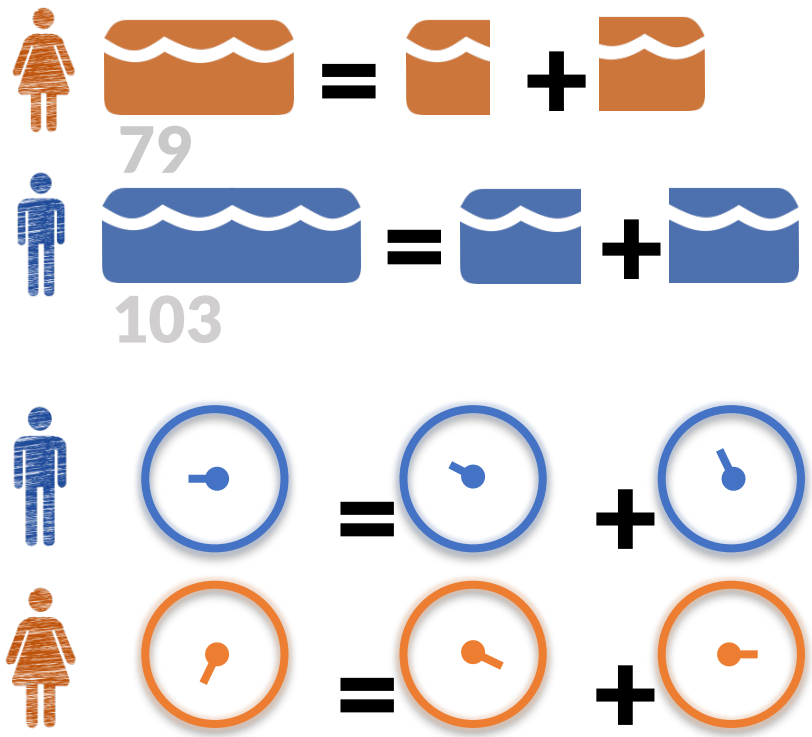
   (a) Generate a secret *random mask* $m_i \in G$ and calcu-
   late the *masked*

   (b) Receive p from

   (c) Send r_i and c_i –

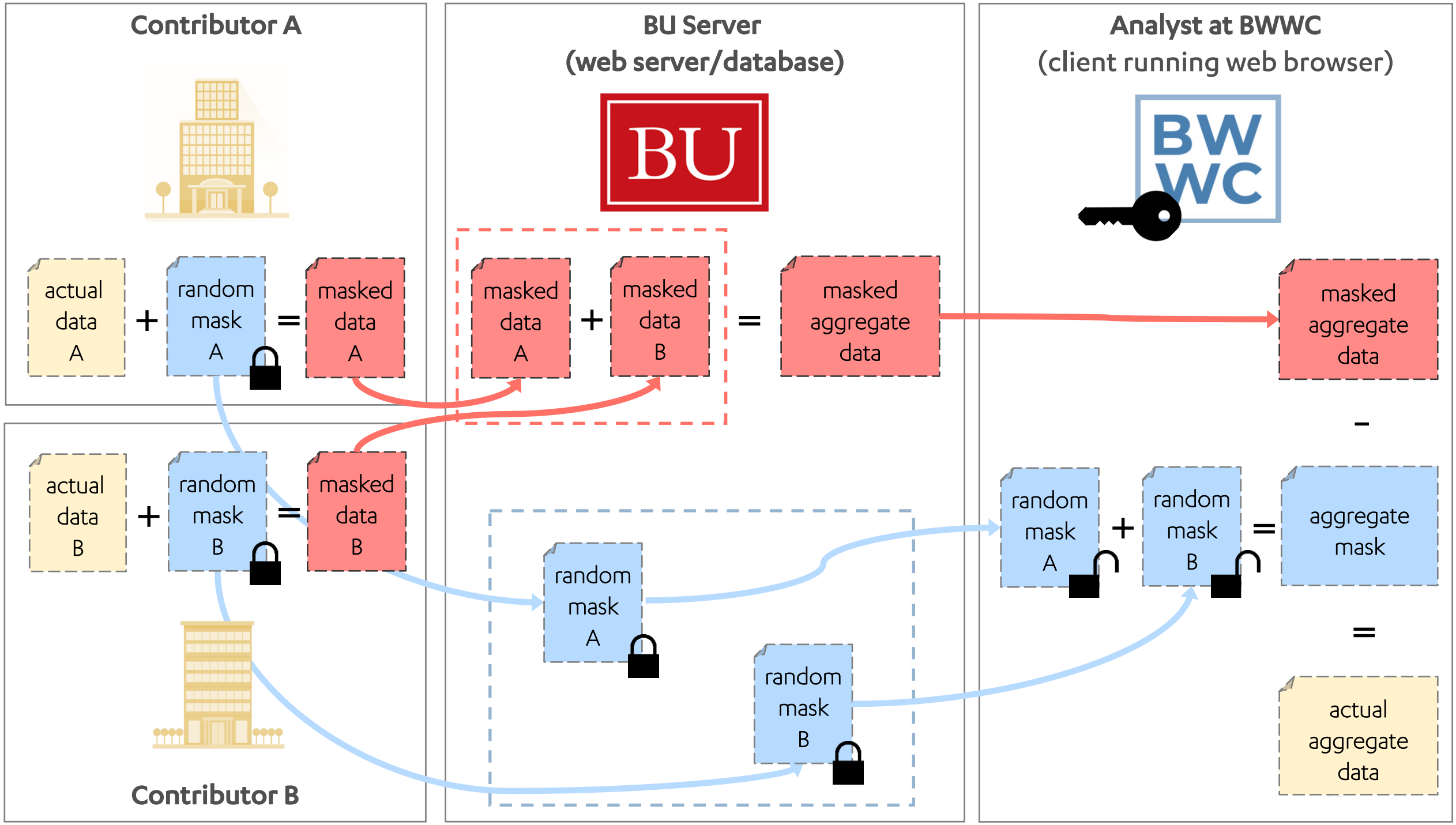
3. The service provider computes the sum of the masked data values to obtain the aggregate masked data quantity $R = \sum_{i=1}^{n} r_i$;

4. The analyst then retrieves R and all the $c_1, \ldots, c_n$ from the service provider, computes $m_i = \mathrm{Dec}_s(c_i)$ 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)
BU
masked data A
+
masked data B
=
masked aggregate data
random mask A
random mask B
Analyst at BWWC
(client running web browser)
BW WC
masked aggregate data
-
random mask A
+
random mask B
=
aggregate mask
=
actual aggregate data

Contributor A

actual data A

actual data B

Contributor B

BU Server
(web server/database)

Analyst at BWWC
(client running web browser)

Contributor A

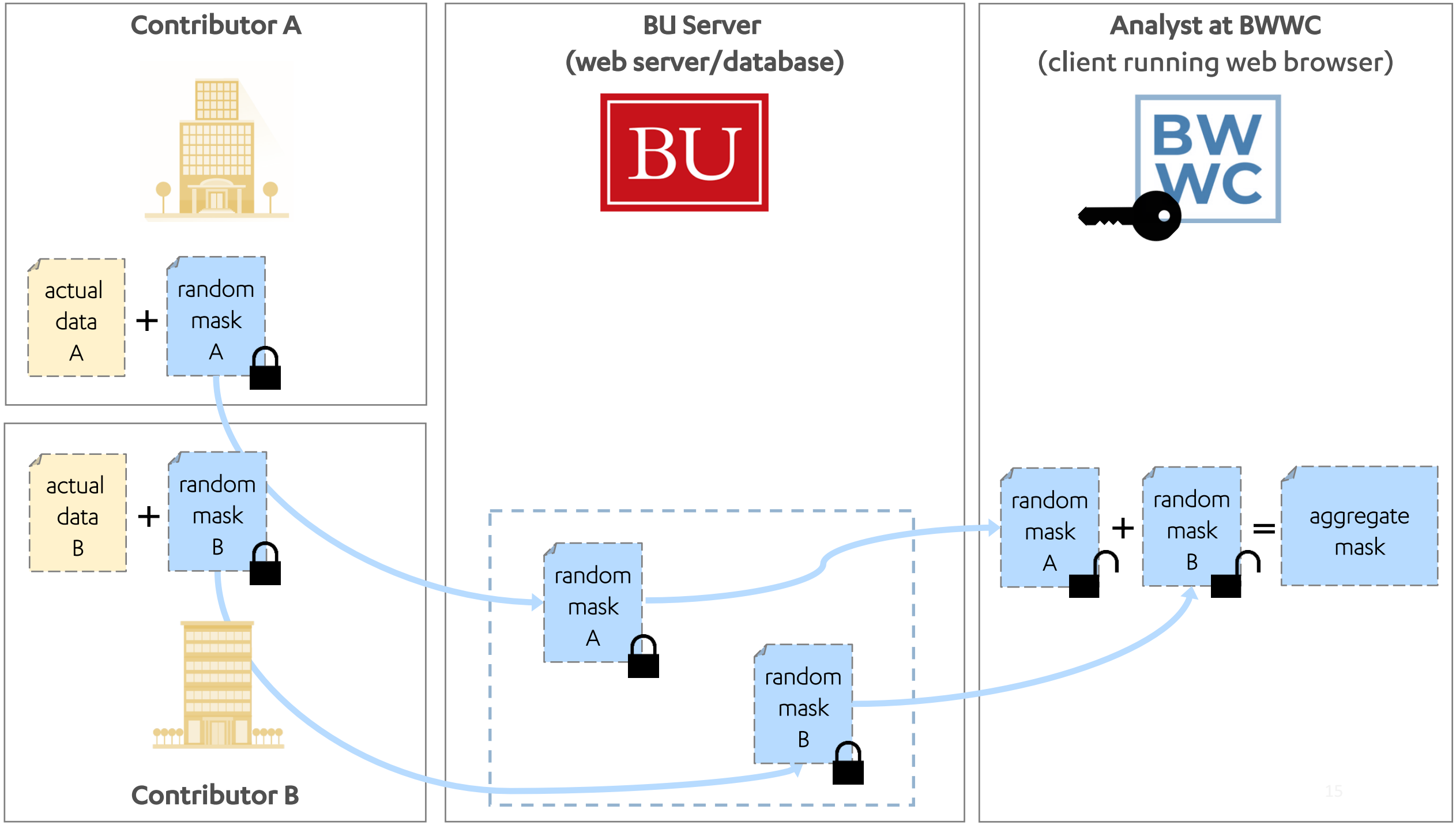
actual data A + random mask A

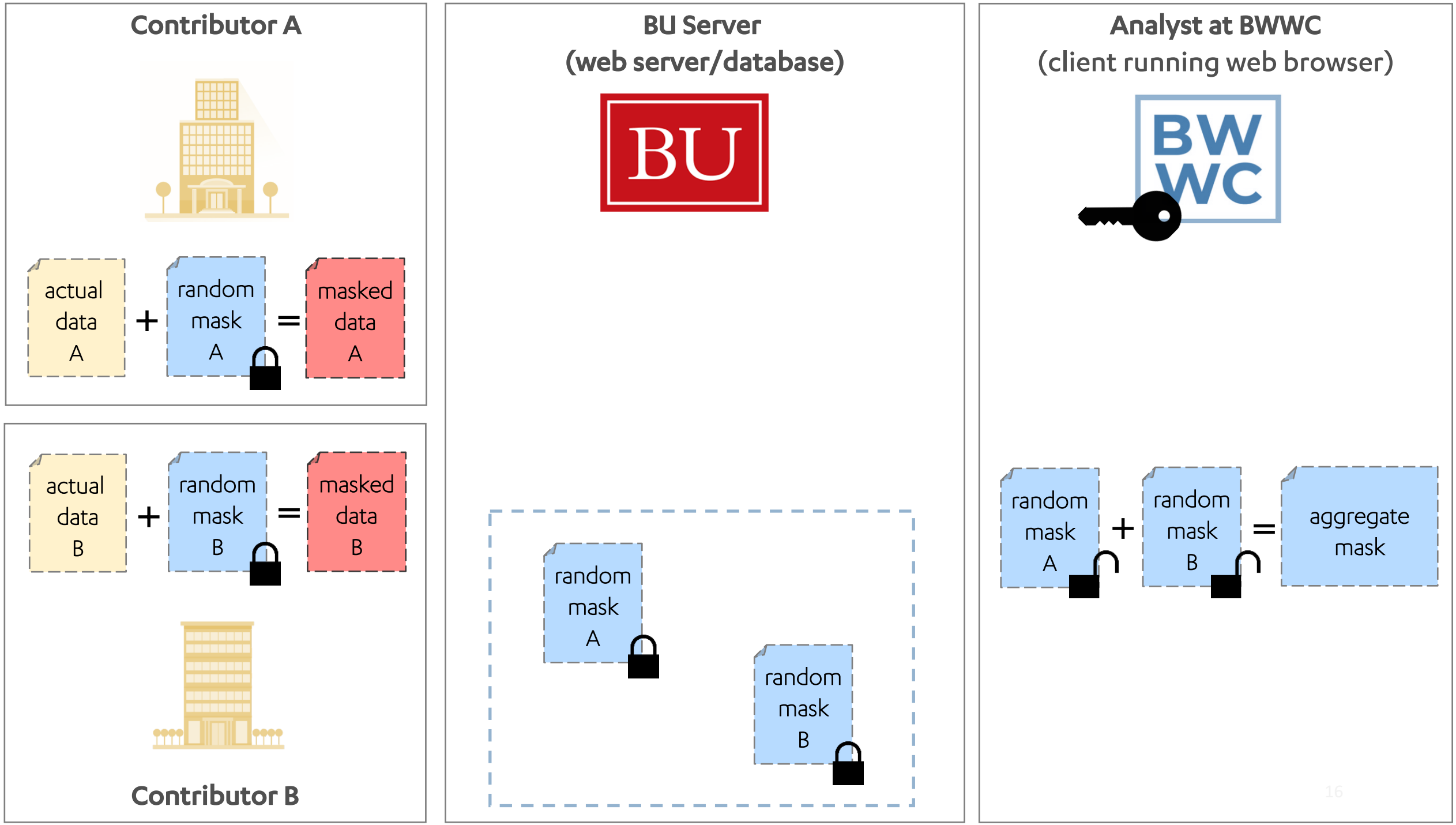
actual data B + random mask B

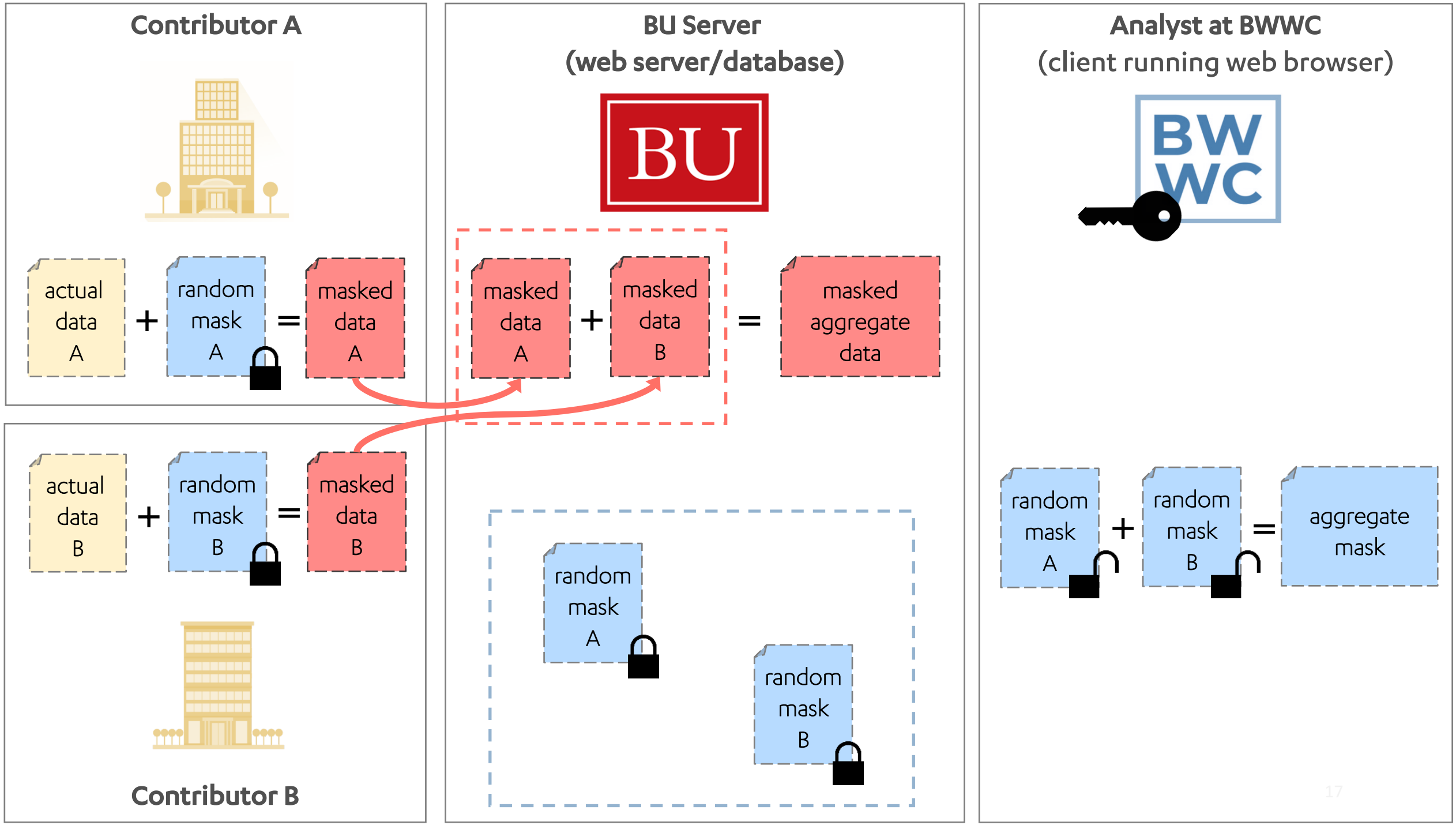
Contributor B

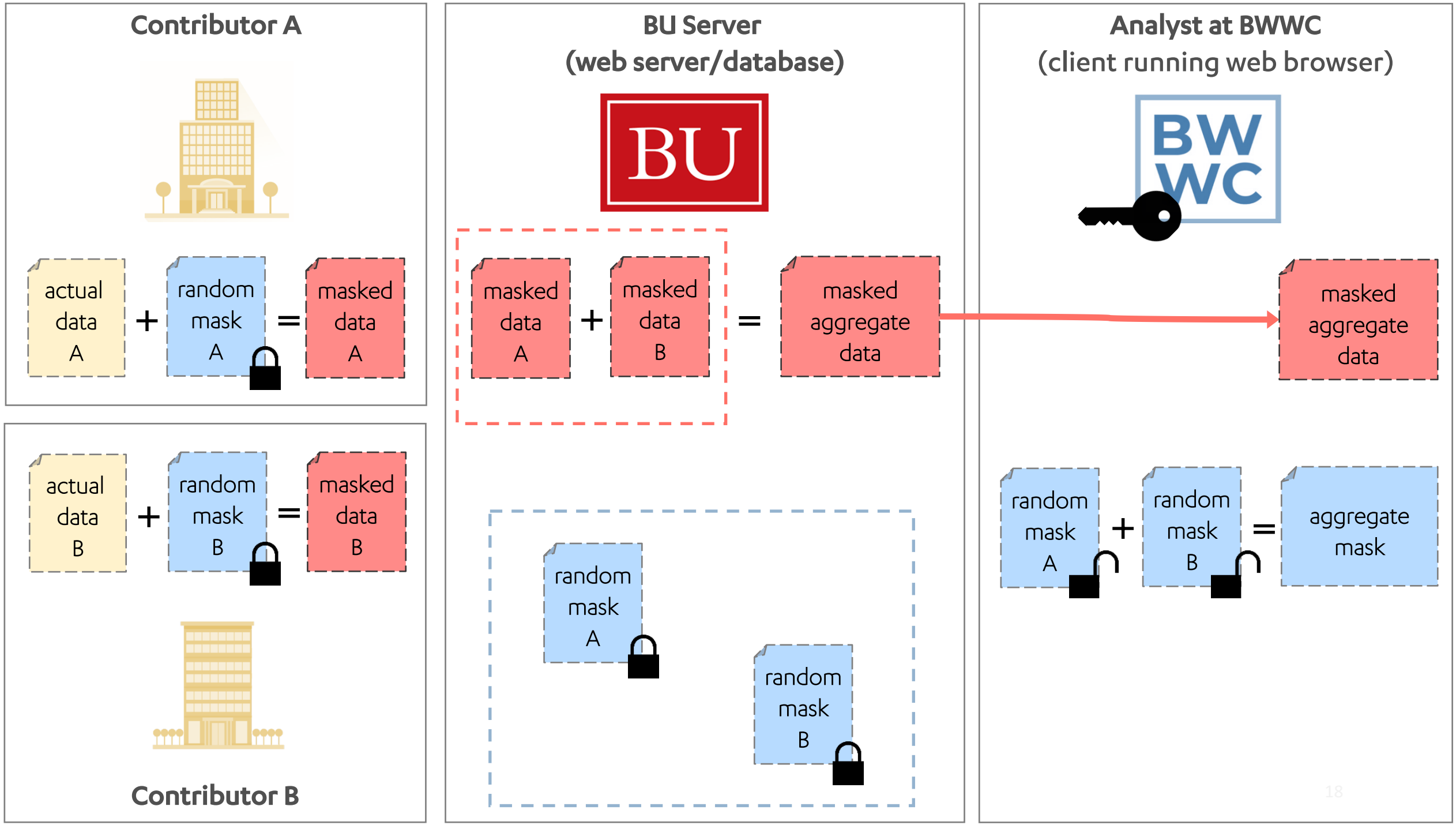
BU Server
(web server/database)

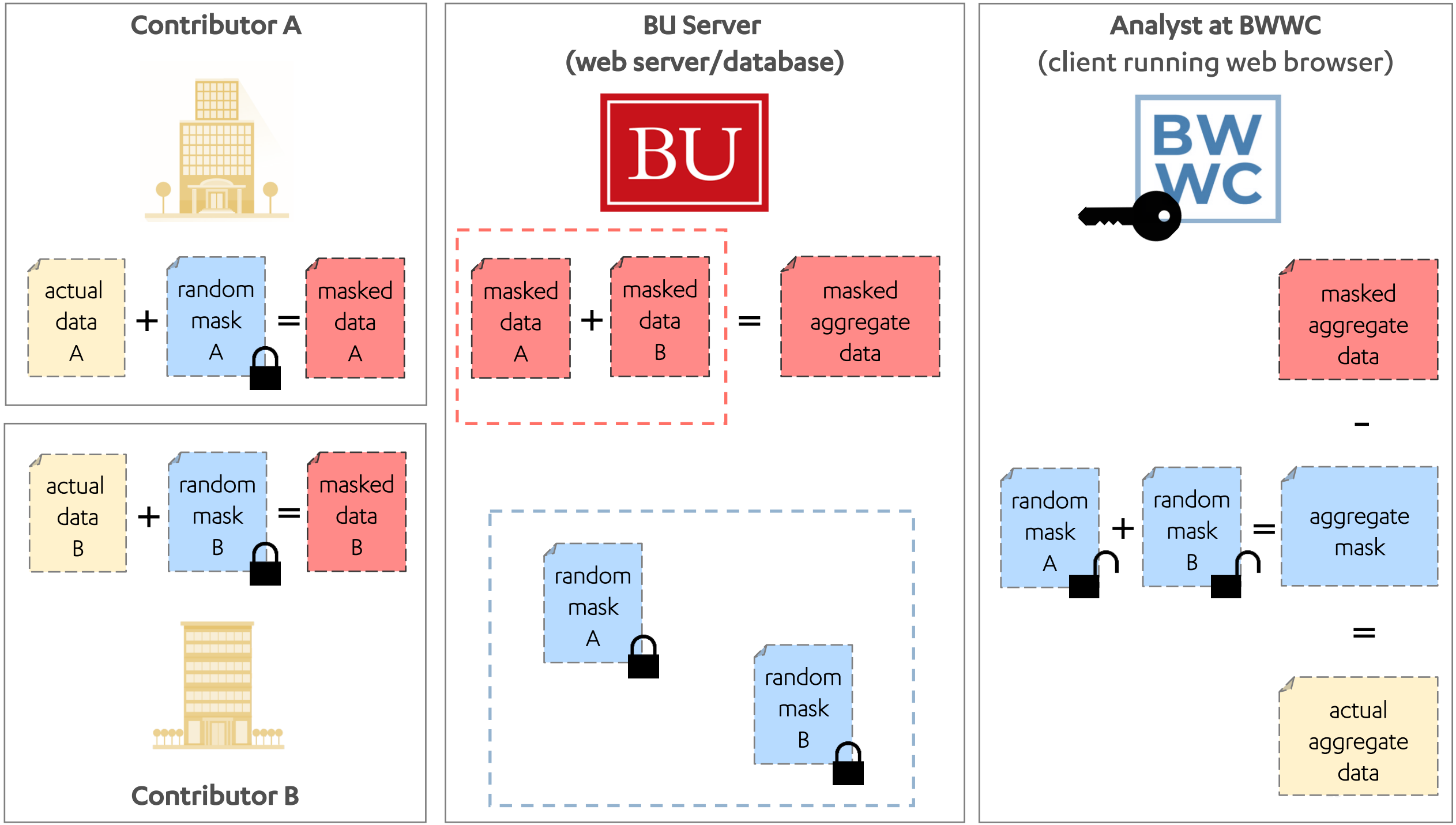
Analyst at BWWC
(client running web browser)


Contributor A
actual data A
+
random mask A
actual data B
+
random mask B
Contributor B
BU Server
(web server/database)
BU
random mask A
random mask B
Analyst at BWWC
(client running web browser)
BW WC
random mask A
+
random mask B
=
aggregate mask


Contributor A
actual data A
+
random mask A
=
masked data A
actual data B
+
random mask B
=
masked data B
Contributor B
BU Server
(web server/database)
BU
random mask A
random mask B
Analyst at BWWC
(client running web browser)
BW WC
random mask A
+
random mask B
=
aggregate mask


Contributor A
actual data A
+
random mask A
=
masked data A
actual data B
+
random mask B
=
masked data B
Contributor B
BU Server
(web server/database)
BU
masked data A
+
masked data B
=
masked aggregate data
random mask A
random mask B
Analyst at BWWC
(client running web browser)
BW WC
random mask A
+
random mask B
=
aggregate mask


Contributor A
actual data A
+
random mask A
=
masked data A
actual data B
+
random mask B
=
masked data B
Contributor B
BU Server
(web server/database)
BU
masked data A
+
masked data B
=
masked aggregate data
random mask A
random mask B
Analyst at BWWC
(client running web browser)
BW WC
masked aggregate data
random mask A
+
random mask B
=
aggregate mask


Contributor A
actual data A
+
random mask A
=
masked data A
actual data B
+
random mask B
=
masked data B
Contributor B
BU Server
(web server/database)
BU
masked data A
+
masked data B
=
masked aggregate data
random mask A
random mask B
Analyst at BWWC
(client running web browser)
BW WC
masked aggregate data
-
random mask A
+
random mask B
=
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

ERROR MINIMIZATION

Asian		American Indian/Alaska Native		Two or More Races (Not Hispanic or Latinx)	
Female	Male	Female	Male	Female	Male
0	0	0	0	0	0
18	10000000	110	111	112	113
28	29				3
38	39				3
48	49	410	411	412	413

Warning: Data is too big

Are you sure this value is correct?

adfs	$47.00	$48.00	$49.00	$410.00	$411.0
$56.00					.0
$66.00					.0
$76.00	$77.00	$78.00	$79.00	$710.00	$711.0

Invalid Data Entry

Please do not input any text or leave any cells blank. If the value is zero, please input zero.

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

	Total Number of Employees		
	Female	Male	All
Total	15905	16390	32295

☐ All data is verified and correct

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

BWWC
BOSTON WOMEN'S WORKFORCE COUNCIL

BOSTON UNIVERSITY

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

dn51w20bdwfbw5yrcvsdr4763w ✔

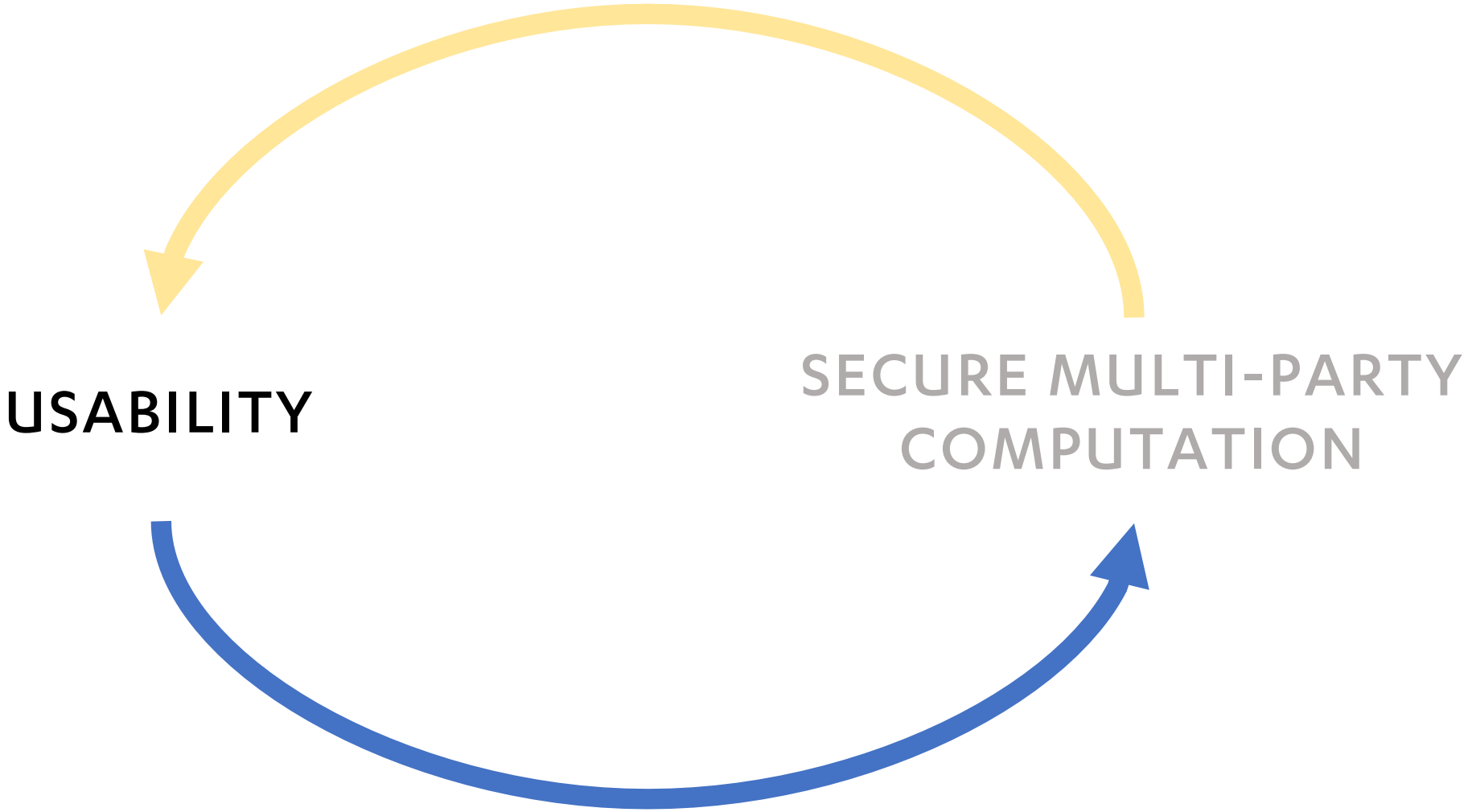
Participation code

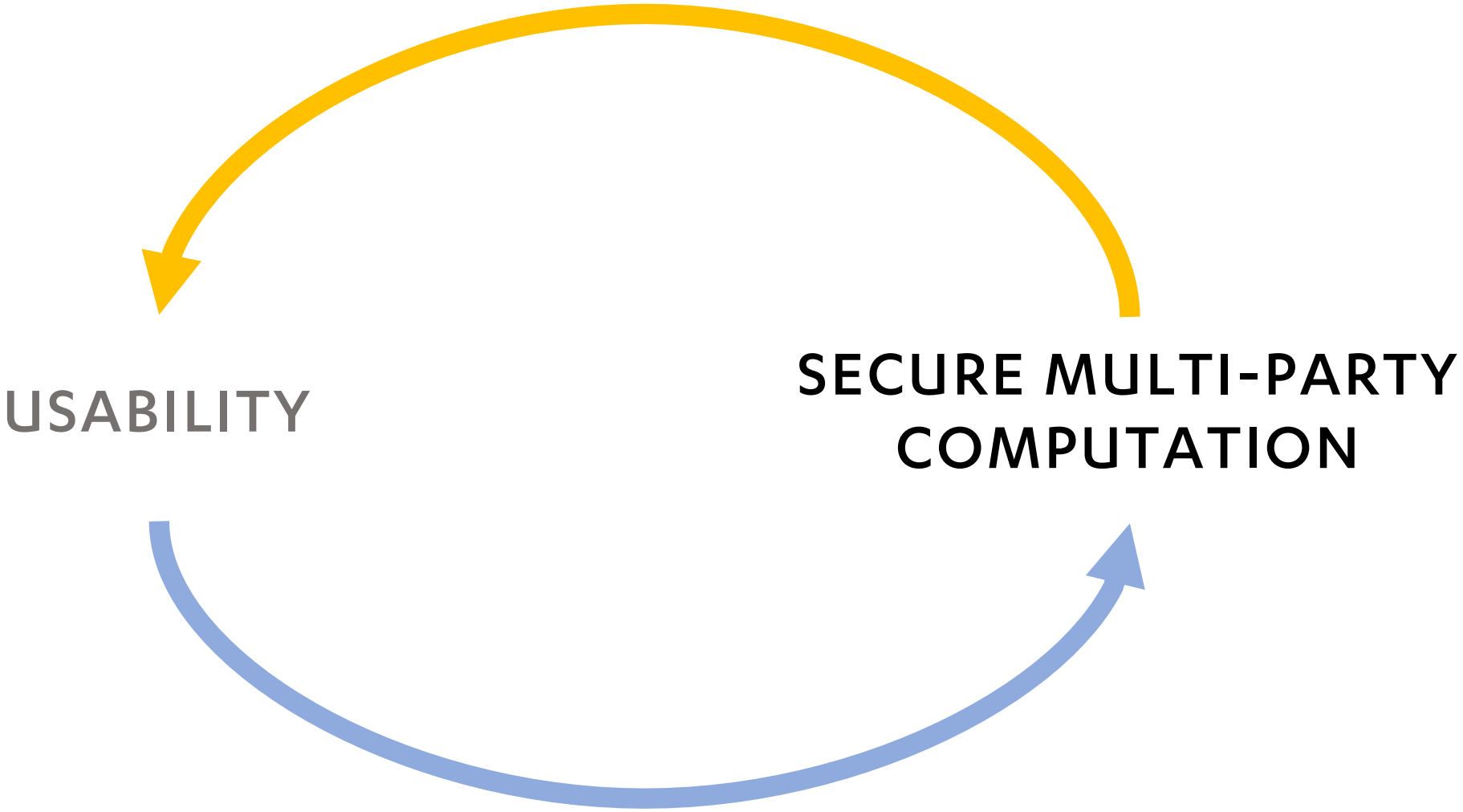
bteq93ckytxrnwmjbsddwh05gr ✔

Drag and drop your completed template file here

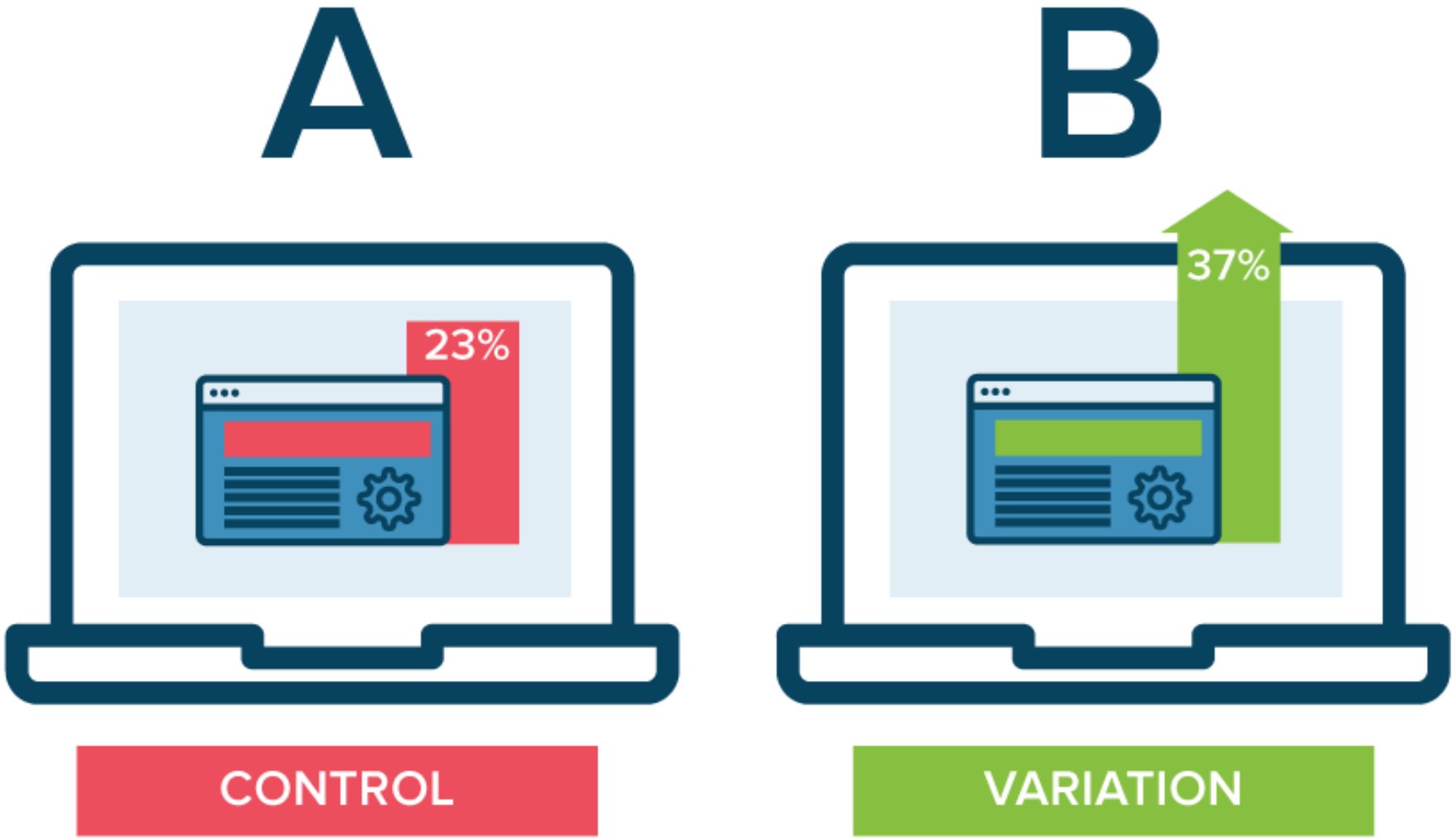
—or—

Choose file

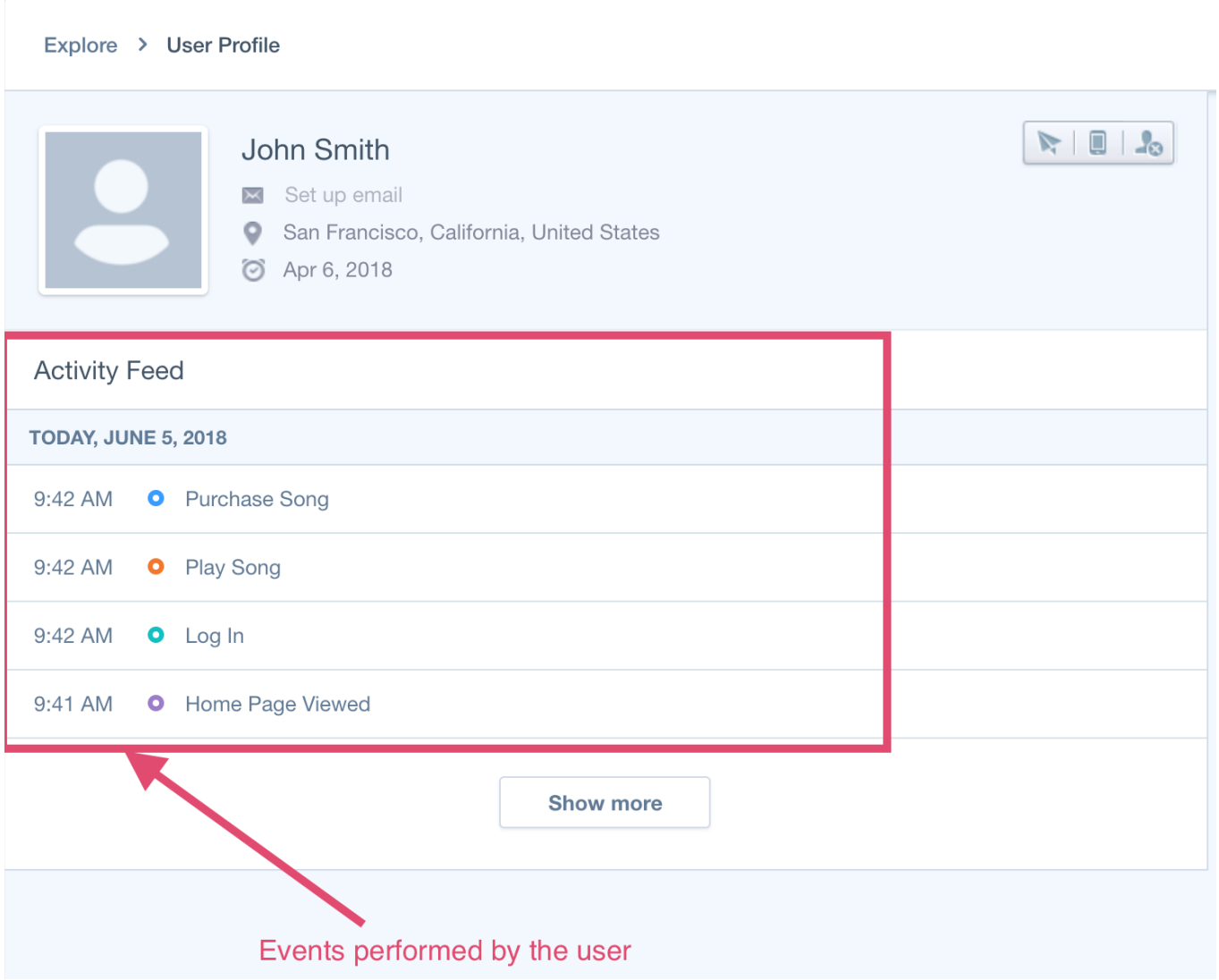

USABILITY
SECURE MULTI-PARTY COMPUTATION

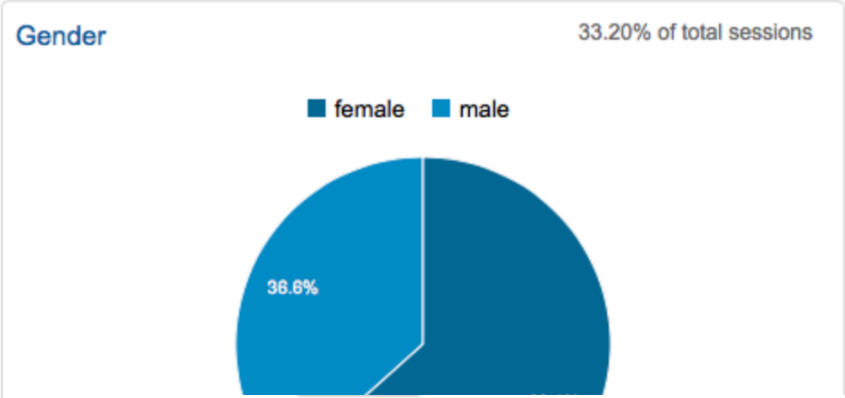

USABILITY
SECURE MULTI-PARTY COMPUTATION

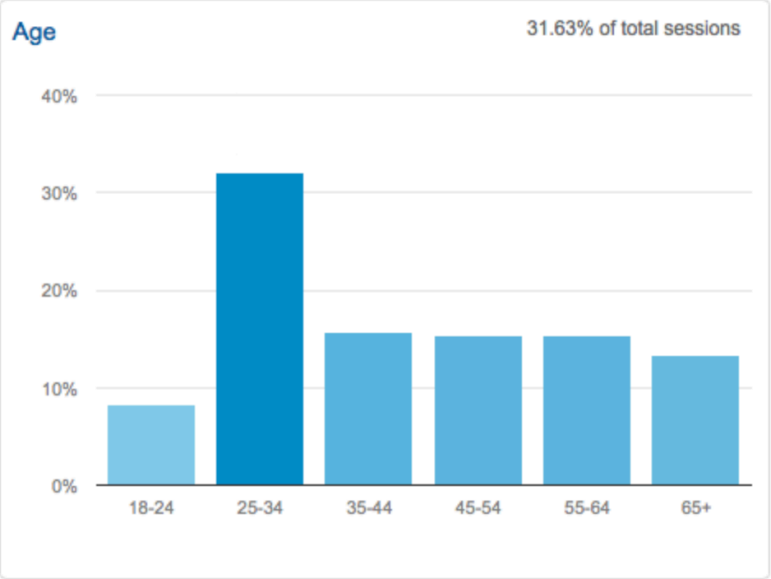
WEB ANALYTICS



WEB ANALYTICS

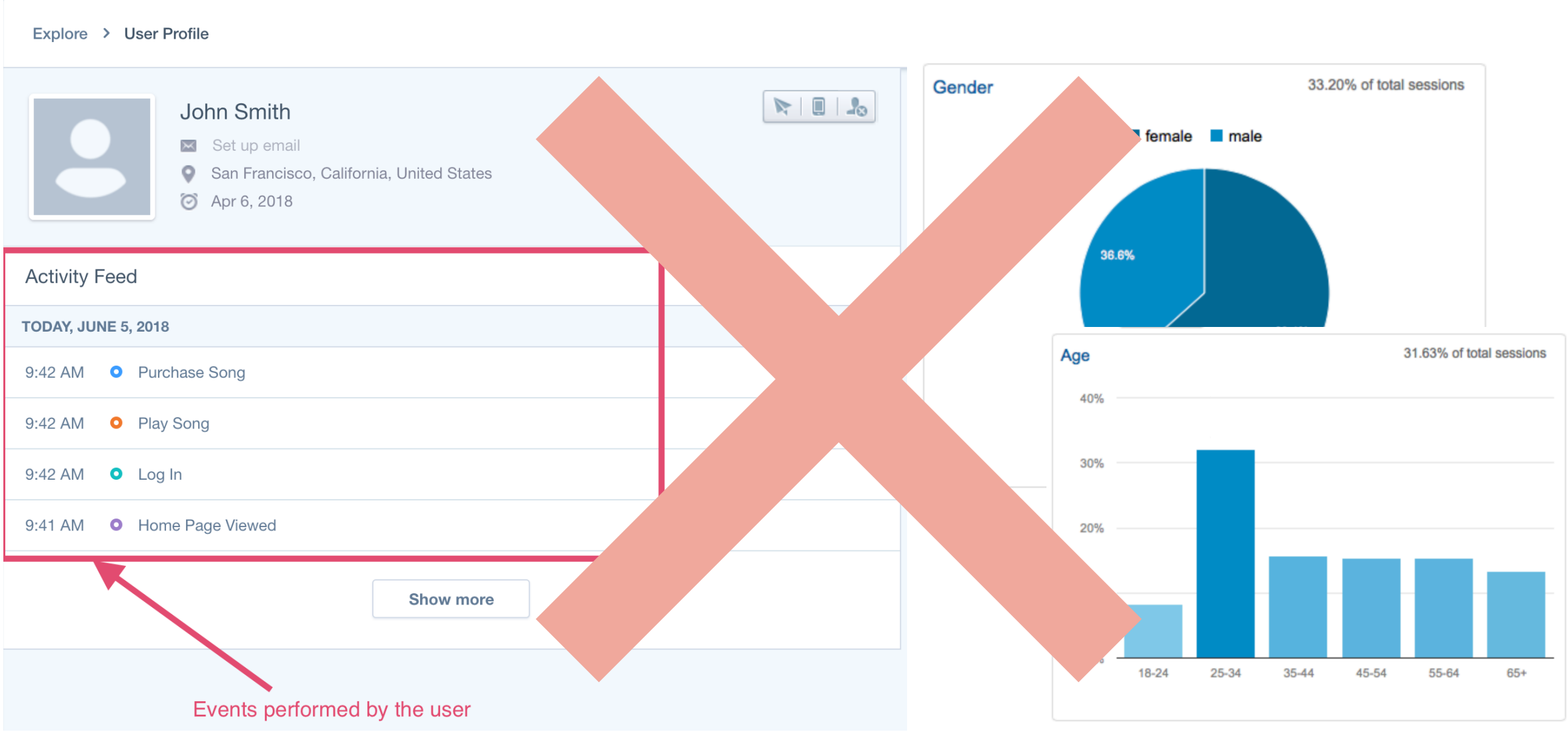






images from Mixpanel and Google Analytics

WEB ANALYTICS



images from Mixpanel and Google Analytics

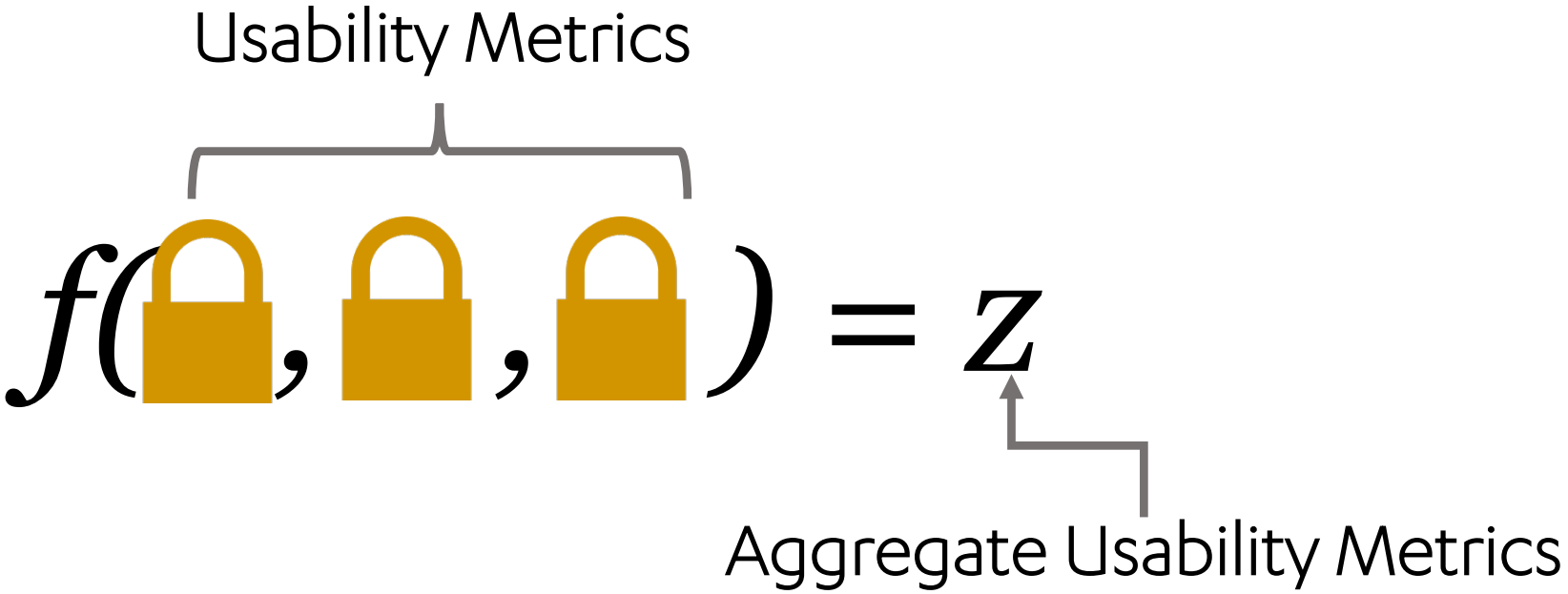
WEB ANALYTICS

mixpanel

Google Analytics

WEB ANALYTICS

REPURPOSING WHAT WE'VE BUILT: **MPC**



USABILITY METRICS UNDER MPC

Browser

Time Spent

UI Feature

Errors

VERSION 1

Enter Session Key

153nk3qwhb39a1g56d89

Enter Participation Code

5sh9q9r2gk60xtk2bb447

Amount Spent with MBEs

	Value for FY in Thousands of Dollars ($)
Dollar Amount Spent with Local MBEs ($)	$11K
Dollar Amount Spent with State MBEs ($)	$52K
Dollar Amount Spent with National MBEs ($)	$23,000,000K

Addressable Spend

	Value for FY18 in Thousands of Dollars
Total Dollar Amount Spent Procuring All Goods and Services Locally ($)	
Total Dollar Amount Spent Procuring All Goods and Services at the State Level ($)	$39K
Total Dollar Amount Spent Procuring All Goods and Services in the United States ($)	$521K

Number of MBEs

	Value for FY18
Number of Local MBEs With Whom You Have Done Business (#)	12
Number of State MBEs With Whom You Have Done Business (#)	56
Number of National MBEs With Whom You Have Done Business (#)	199

☐ All numbers are verified and correct

Submit

VERSION 2

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

	Value for FY18 in Thousands of Dollars
Dollar Amount Spent with Local MBEs	$10,000K
Dollar Amount Spent with State MBEs	$920K
Dollar Amount Spent with National MBEs	K

Invalid Data Entry

Please do not input any text or leave any cells blank. If the value is zero, please input zero.

Addressable Spend

	Value for FY18 in Thousands of Dollars
Total Dollar Amount Spent Procuring All Goods and Services Locally	
Total Dollar Amount Spent Procuring All Goods and Services at the State Level	
Total Dollar Amount Spent Procuring All Goods and Services in the United States	

Number of MBEs

	Value for FY18
Number of Local MBEs With Whom You Have Done Business	
Number of State MBEs With Whom You Have Done Business	
Number of National MBEs With Whom You Have Done Business	

VERSION 3

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

Session key

Participation code

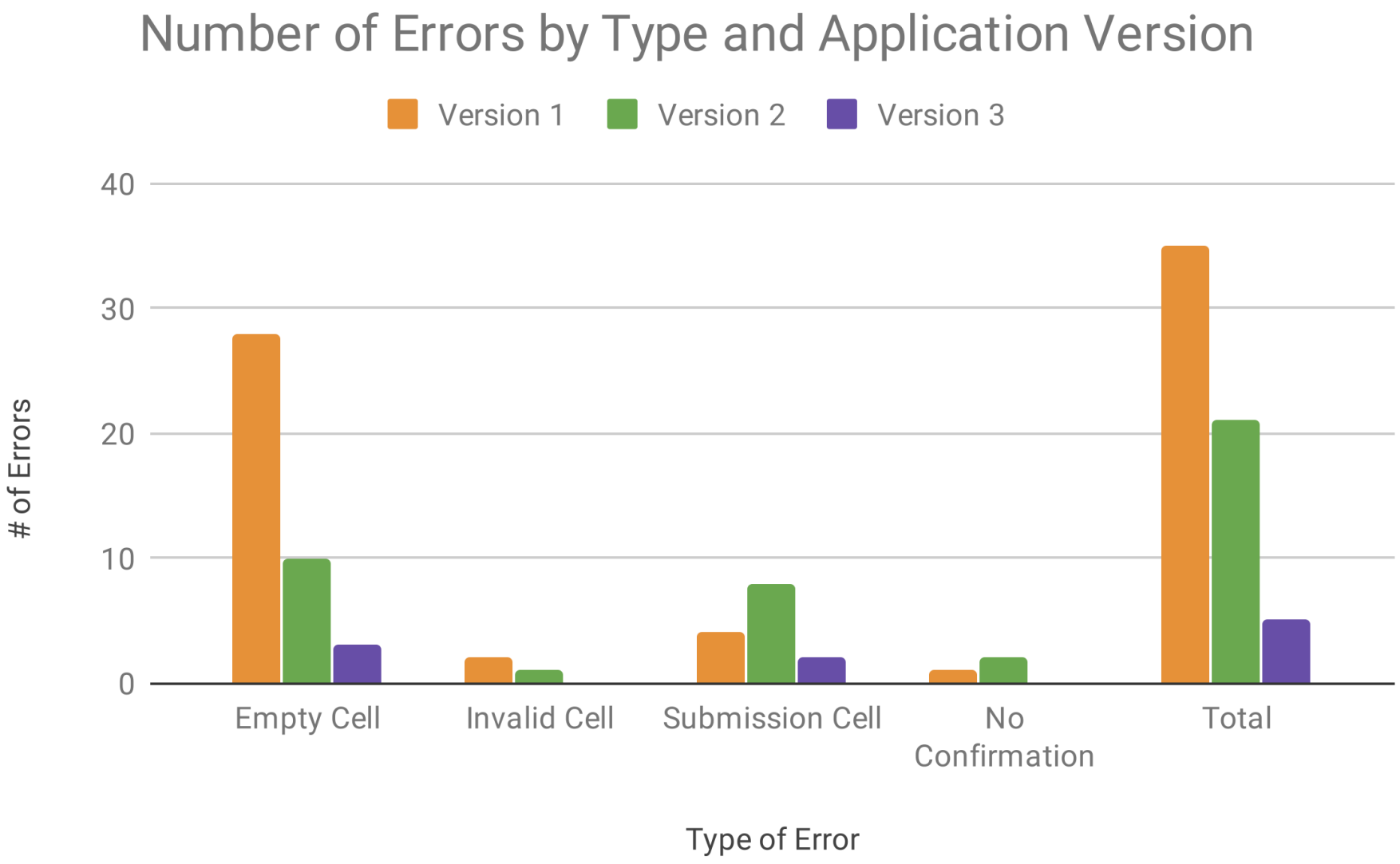
Participation code

Drag and drop your completed template file here

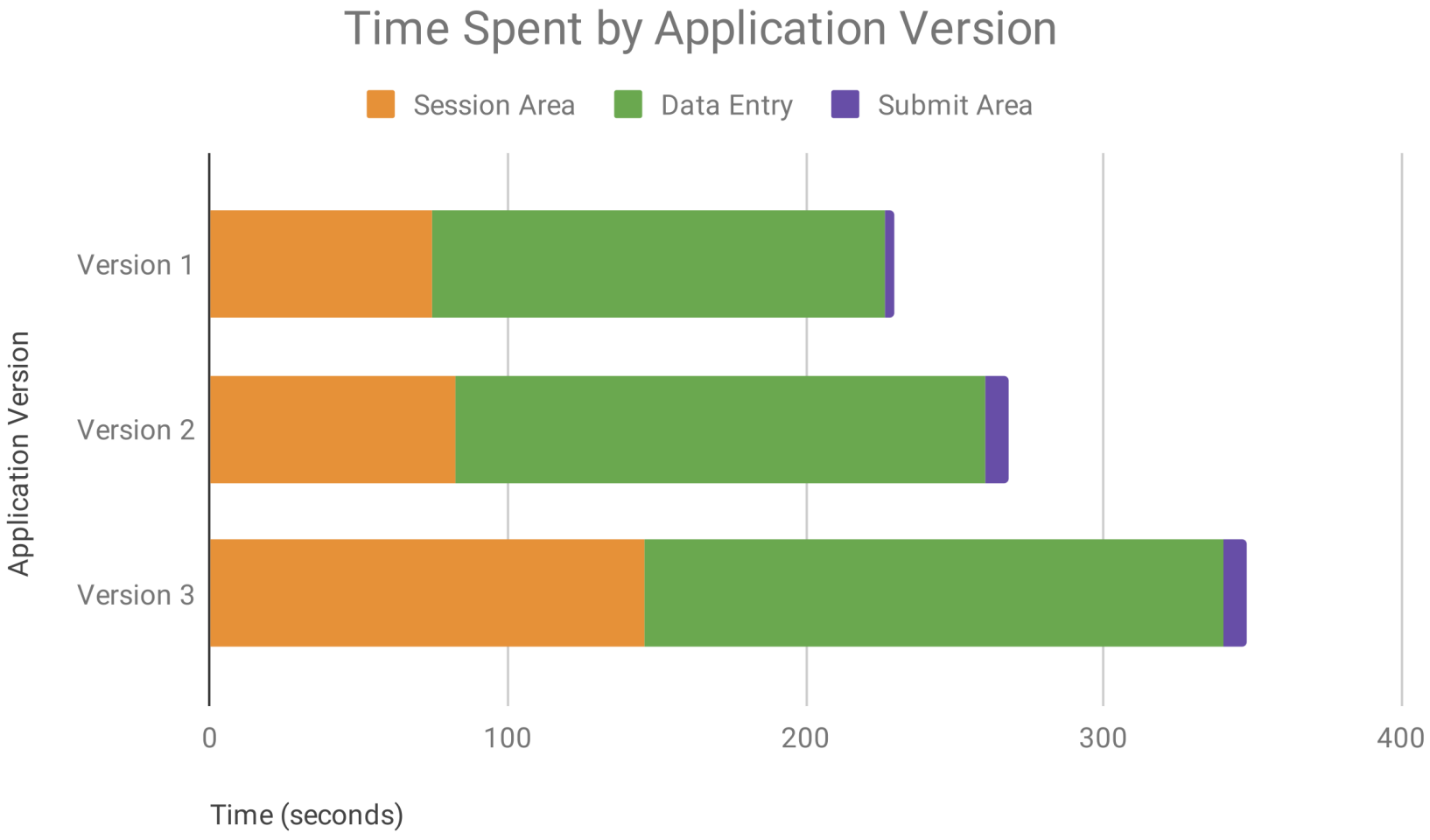
—or—

Choose file

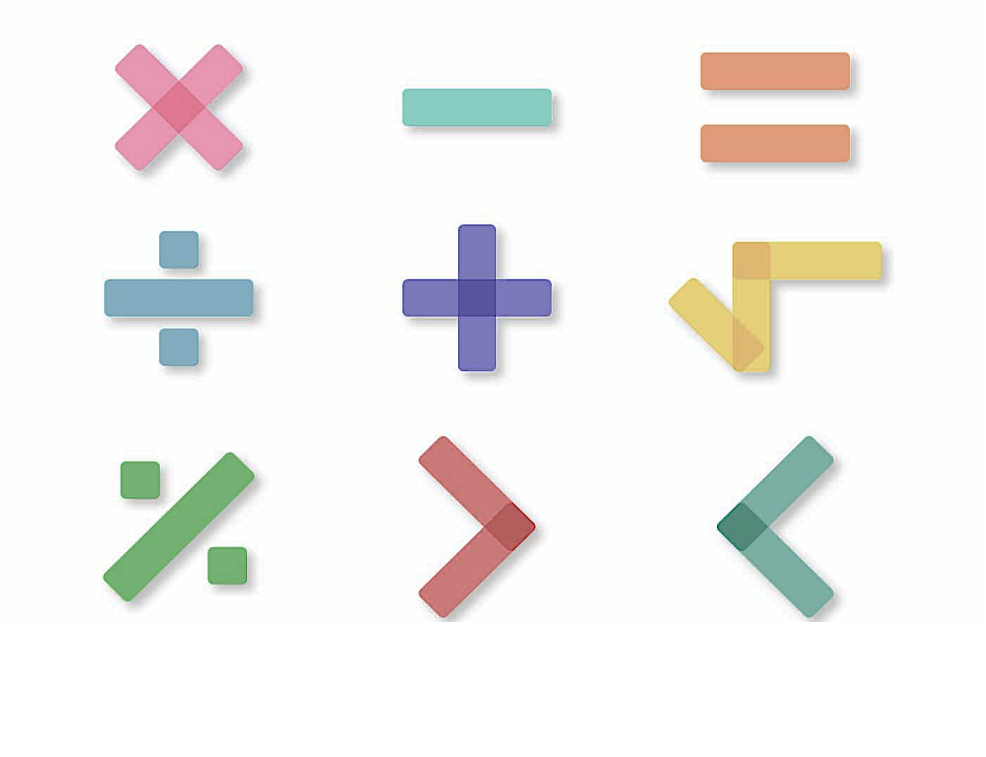
RESULTS FROM USABILITY STUDY



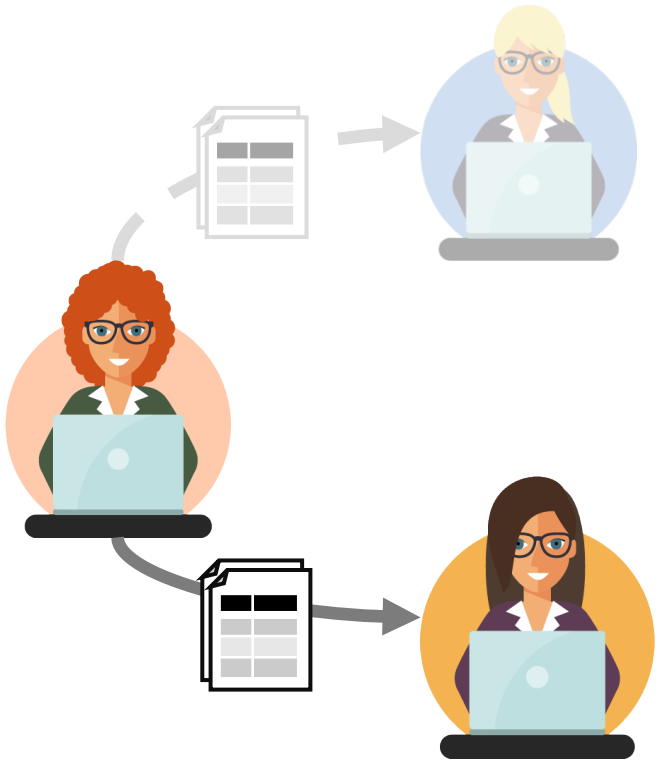
RESULTS FROM USABILITY STUDY



LIMITATIONS



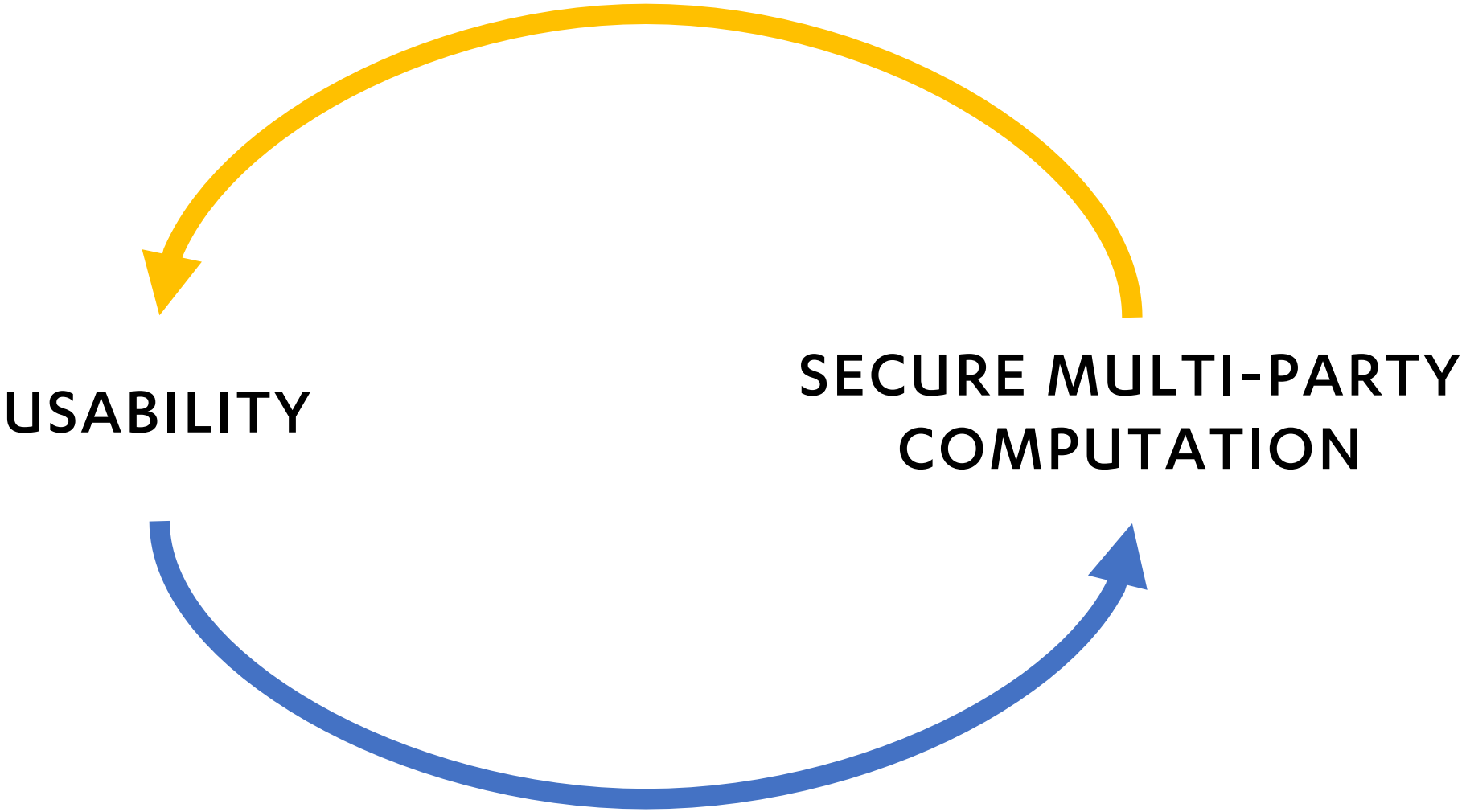
limited statistics



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

BWWC
BOSTON WOMEN'S WORKFORCE COUNCIL

HRI
Honda Research Institute

Greater Boston
Chamber of Commerce

NSF

lucyq@brown.edu
pflock@bu.edu

/multiparty/**web-mpc**
/multiparty/**jiff**

multiparty.org

MPC WORKFLOW