Lecture 21: Applications of protected computing

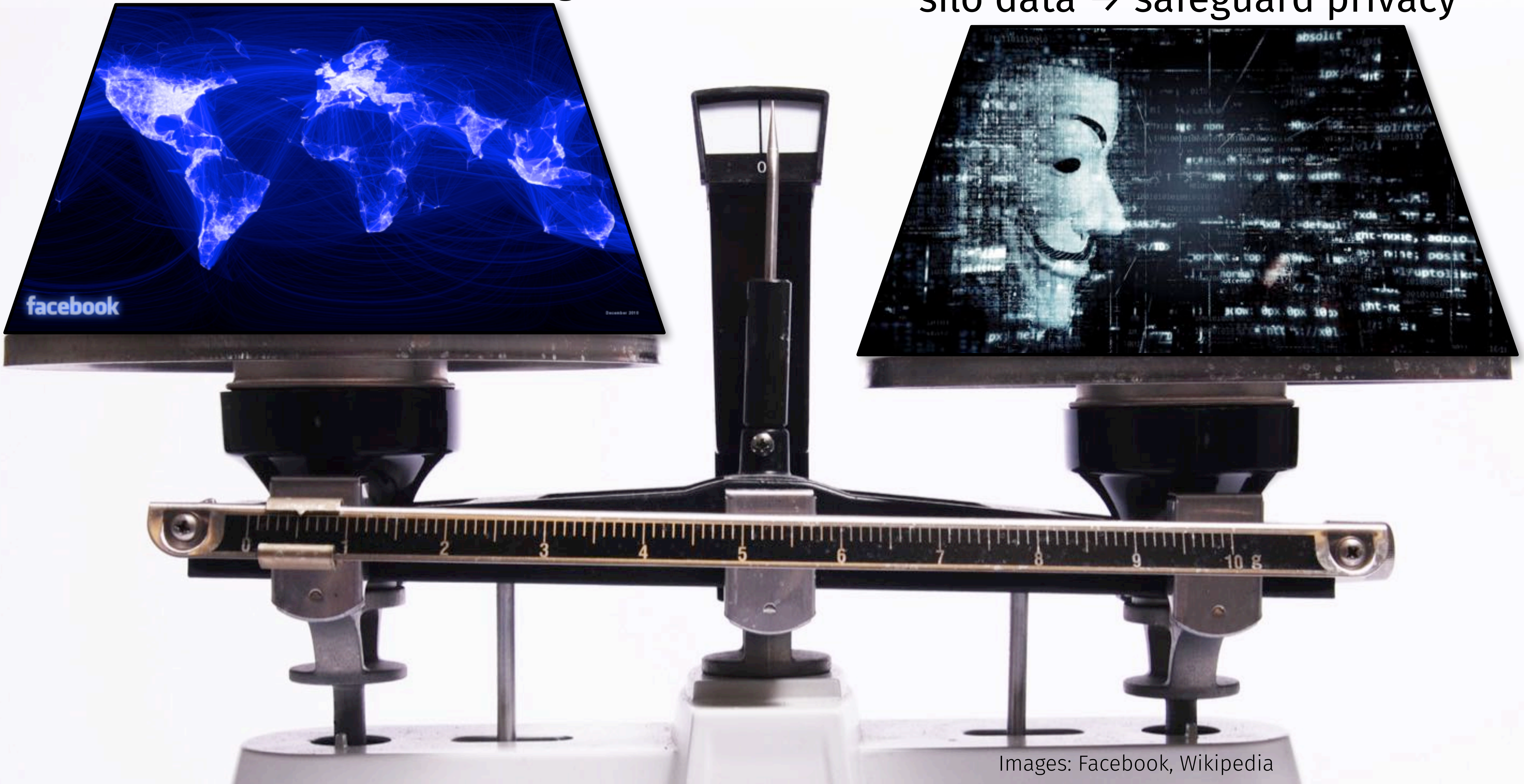
- Lab 11 due Wednesday 5/1
- Online course evaluation is live at bu.campuslabs.com/courseeval
- Thursday office hours: 12-1pm and 3-5pm
- Final exam
  - Scope: all topics covered in lectures, recitations, and labs (except law/policy)
  - Sample final exam has been posted on Piazza
  - Final exam review session is on Saturday 5/3 at 3-5pm (location TBD)

Data is valuable

share data → new social insights

Data is toxic

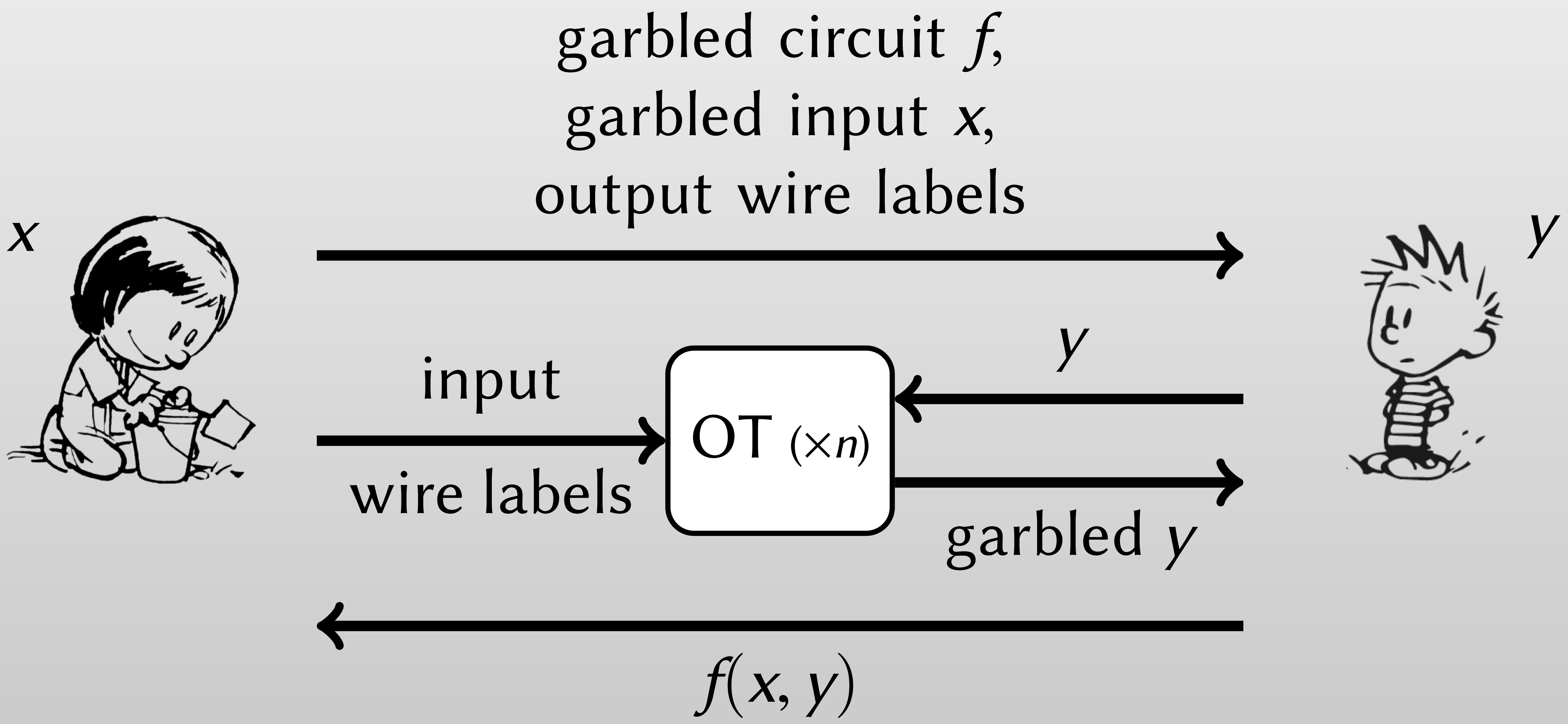
silo data → safeguard privacy



Images: Facebook, Wikipedia

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

Yao’s Protocol: overview



x

garbled circuit f,
garbled input x,
output wire labels

y

input wire labels

OT $(\times n)$

y

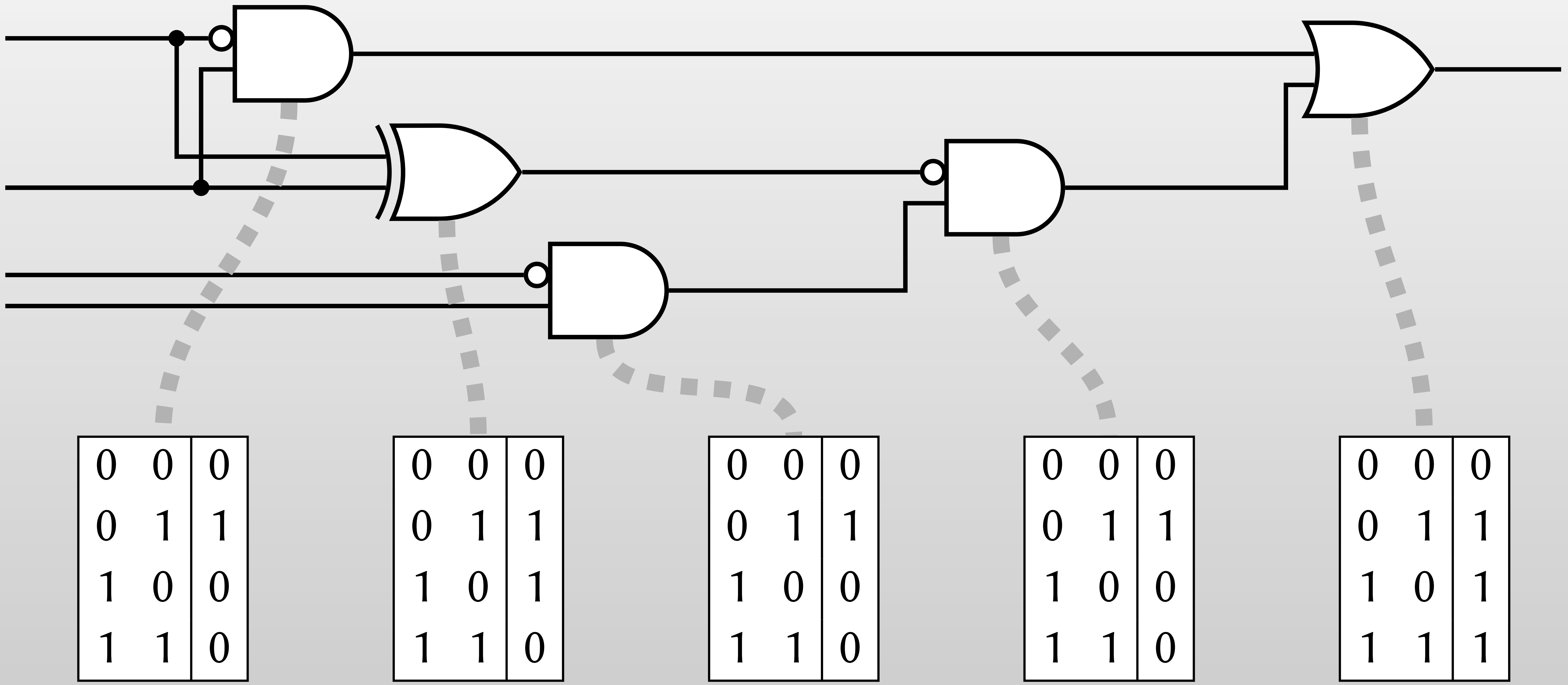
garbled y

$f(x, y)$

- Given garbled f + garbled inputs + all output labels $\Rightarrow$ Bob learns **only** $f(x, y)$

Slides by Mike Rosulek, OSU

Garbled circuit framework [Yao86]



0	0	0
0	1	1
1	0	0
1	1	0

0	0	0
0	1	1
1	0	1
1	1	0

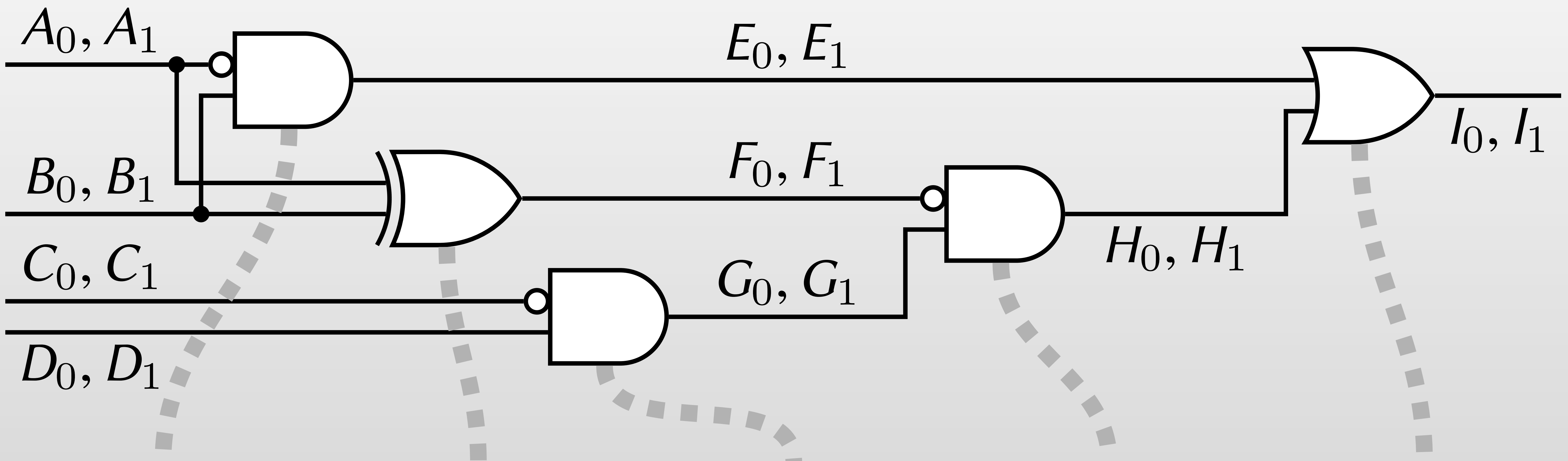
0	0	0
0	1	1
1	0	0
1	1	0

0	0	0
0	1	1
1	0	0
1	1	0

0	0	0
0	1	1
1	0	1
1	1	1

Slides by Mike Rosulek, OSU

Garbled circuit framework [Yao86]



A_0	B_0	E_0
A_0	B_1	E_1
A_1	B_0	E_0
A_1	B_1	E_0

A_0	B_0	F_0
A_0	B_1	F_1
A_1	B_0	F_1
A_1	B_1	F_0

C_0	D_0	G_0
C_0	D_1	G_1
C_1	D_0	G_0
C_1	D_1	G_0

F_0	G_0	H_0
F_0	G_1	H_1
F_1	G_0	H_0
F_1	G_1	H_0

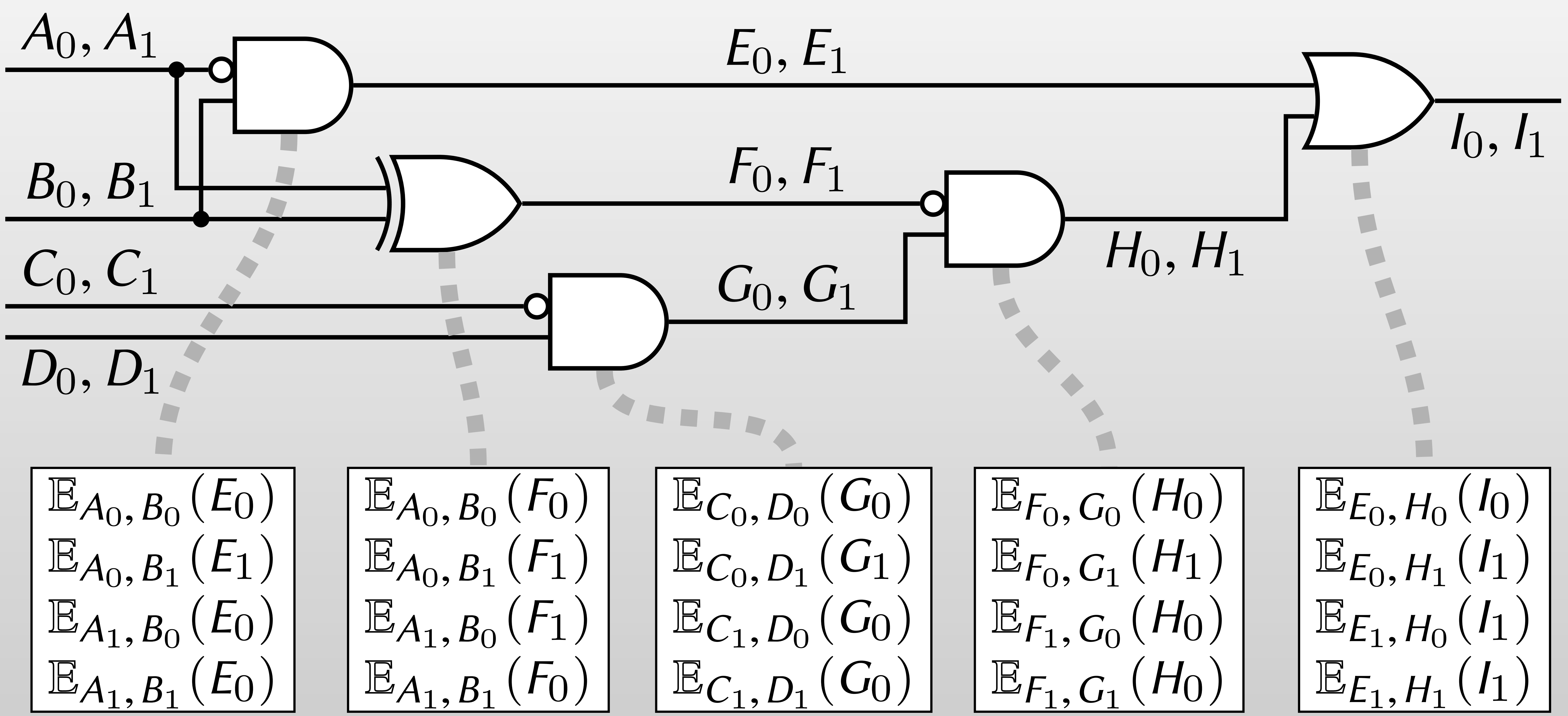
E_0	H_0	I_0
E_0	H_1	I_1
E_1	H_0	I_1
E_1	H_1	I_1

Garbling a circuit:

- Pick random **labels** W_0, W_1 on each wire

Slides by Mike Rosulek, OSU

Garbled circuit framework [Yao86]



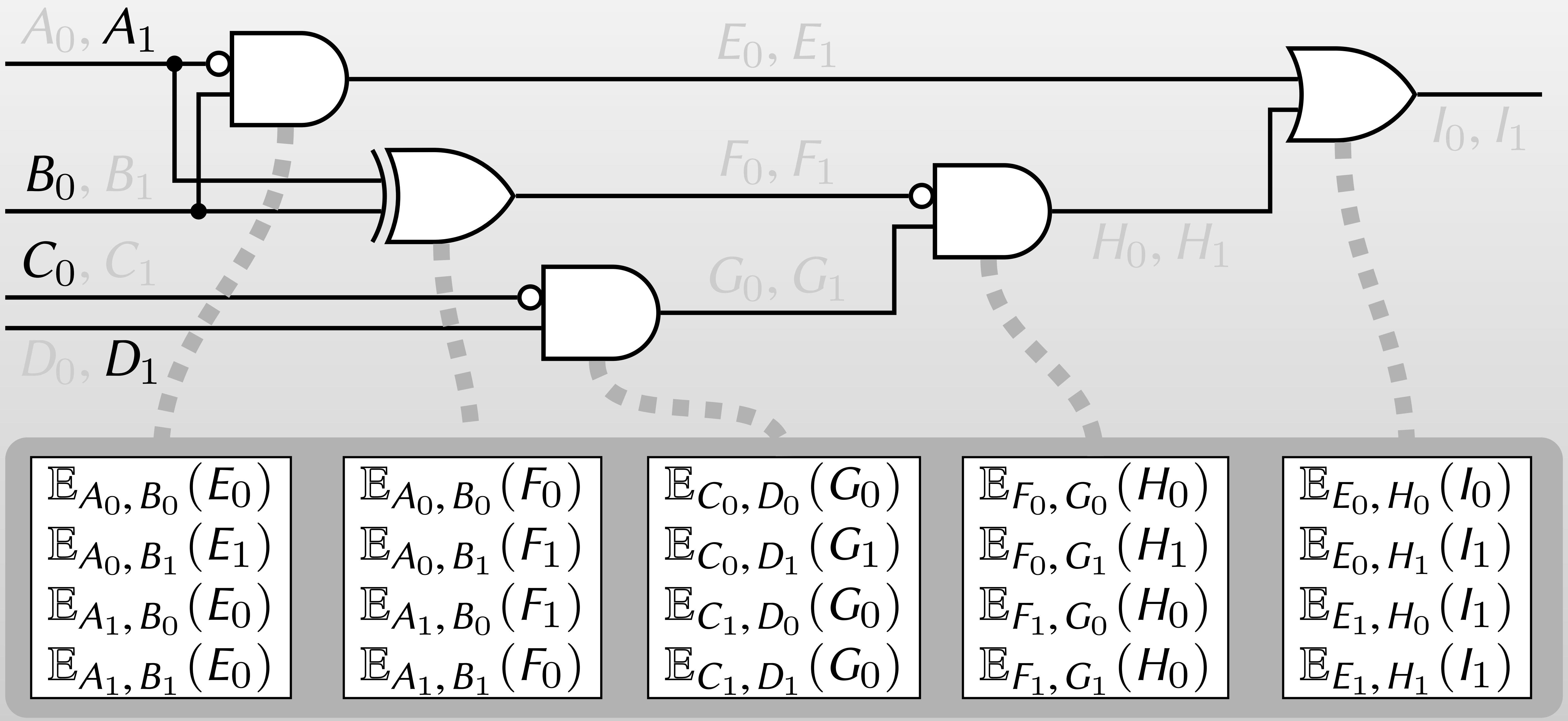
$\mathbb{E}_{A_0,B_0}(E_0)$	$\mathbb{E}_{A_0,B_0}(F_0)$	$\mathbb{E}_{C_0,D_0}(G_0)$	$\mathbb{E}_{F_0,G_0}(H_0)$	$\mathbb{E}_{E_0,H_0}(I_0)$
$\mathbb{E}_{A_0,B_1}(E_1)$	$\mathbb{E}_{A_0,B_1}(F_1)$	$\mathbb{E}_{C_0,D_1}(G_1)$	$\mathbb{E}_{F_0,G_1}(H_1)$	$\mathbb{E}_{E_0,H_1}(I_1)$
$\mathbb{E}_{A_1,B_0}(E_0)$	$\mathbb{E}_{A_1,B_0}(F_1)$	$\mathbb{E}_{C_1,D_0}(G_0)$	$\mathbb{E}_{F_1,G_0}(H_0)$	$\mathbb{E}_{E_1,H_0}(I_1)$
$\mathbb{E}_{A_1,B_1}(E_0)$	$\mathbb{E}_{A_1,B_1}(F_0)$	$\mathbb{E}_{C_1,D_1}(G_0)$	$\mathbb{E}_{F_1,G_1}(H_0)$	$\mathbb{E}_{E_1,H_1}(I_1)$

Garbling a circuit:

- Pick random **labels** W_0, W_1 on each wire
- “Encrypt” truth table of each gate

Slides by Mike Rosulek, OSU

Garbled circuit framework [Yao86]



$\mathbb{E}_{A_0,B_0}(E_0)$
$\mathbb{E}_{A_0,B_1}(E_1)$
$\mathbb{E}_{A_1,B_0}(E_0)$
$\mathbb{E}_{A_1,B_1}(E_0)$

$\mathbb{E}_{A_0,B_0}(F_0)$
$\mathbb{E}_{A_0,B_1}(F_1)$
$\mathbb{E}_{A_1,B_0}(F_1)$
$\mathbb{E}_{A_1,B_1}(F_0)$

$\mathbb{E}_{C_0,D_0}(G_0)$
$\mathbb{E}_{C_0,D_1}(G_1)$
$\mathbb{E}_{C_1,D_0}(G_0)$
$\mathbb{E}_{C_1,D_1}(G_0)$

$\mathbb{E}_{F_0,G_0}(H_0)$
$\mathbb{E}_{F_0,G_1}(H_1)$
$\mathbb{E}_{F_1,G_0}(H_0)$
$\mathbb{E}_{F_1,G_1}(H_0)$

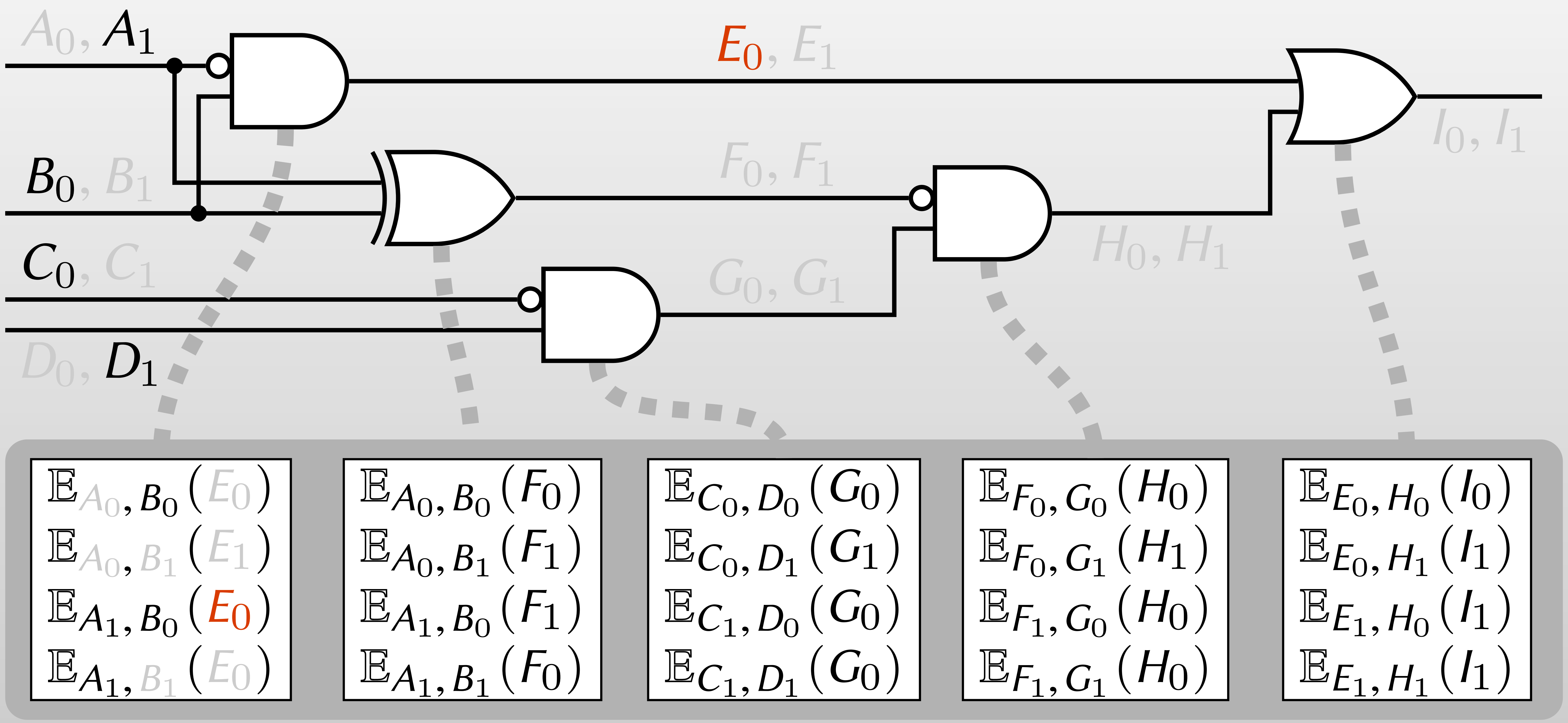
$\mathbb{E}_{E_0,H_0}(I_0)$
$\mathbb{E}_{E_0,H_1}(I_1)$
$\mathbb{E}_{E_1,H_0}(I_1)$
$\mathbb{E}_{E_1,H_1}(I_1)$

Garbling a circuit:

- Pick random **labels** W_0, W_1 on each wire
- "Encrypt" truth table of each gate
- **Garbled circuit** ≡ all encrypted gates
- **Garbled encoding** ≡ one label per wire

Slides by Mike Rosulek, OSU

Garbled circuit framework [Yao86]



$\mathbb{E}_{A_0,B_0}(E_0)$	$\mathbb{E}_{A_0,B_0}(F_0)$	$\mathbb{E}_{C_0,D_0}(G_0)$	$\mathbb{E}_{F_0,G_0}(H_0)$	$\mathbb{E}_{E_0,H_0}(I_0)$
$\mathbb{E}_{A_0,B_1}(E_1)$	$\mathbb{E}_{A_0,B_1}(F_1)$	$\mathbb{E}_{C_0,D_1}(G_1)$	$\mathbb{E}_{F_0,G_1}(H_1)$	$\mathbb{E}_{E_0,H_1}(I_1)$
$\mathbb{E}_{A_1,B_0}(E_0)$	$\mathbb{E}_{A_1,B_0}(F_1)$	$\mathbb{E}_{C_1,D_0}(G_0)$	$\mathbb{E}_{F_1,G_0}(H_0)$	$\mathbb{E}_{E_1,H_0}(I_1)$
$\mathbb{E}_{A_1,B_1}(E_0)$	$\mathbb{E}_{A_1,B_1}(F_0)$	$\mathbb{E}_{C_1,D_1}(G_0)$	$\mathbb{E}_{F_1,G_1}(H_0)$	$\mathbb{E}_{E_1,H_1}(I_1)$

Garbling a circuit:

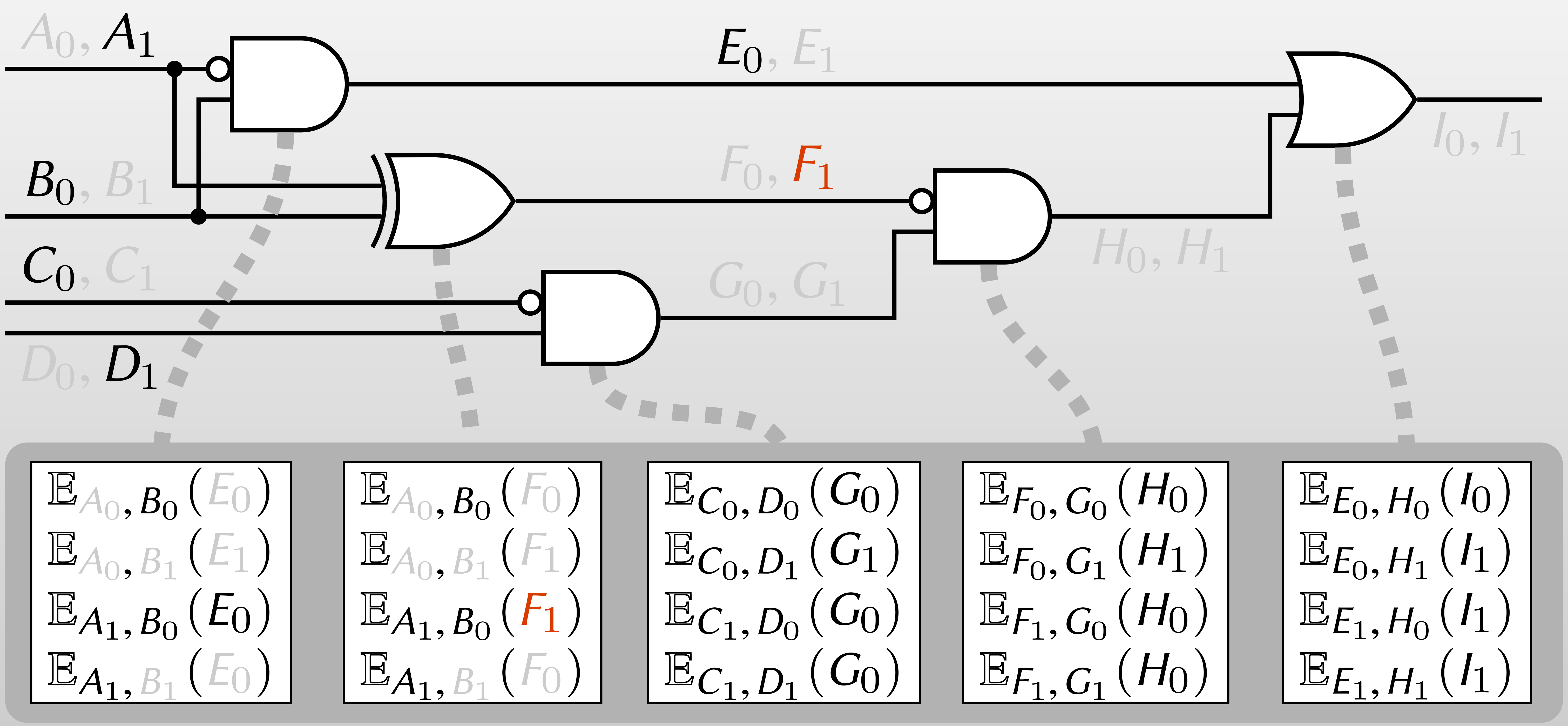
- Pick random **labels** W_0, W_1 on each wire
- “Encrypt” truth table of each gate
- **Garbled circuit** ≡ all encrypted gates
- **Garbled encoding** ≡ one label per wire

Garbled evaluation:

- Only one ciphertext per gate is decryptable

Slides by Mike Rosulek, OSU

Garbled circuit framework [Yao86]



$\mathbb{E}_{A_0,B_0}(E_0)$	$\mathbb{E}_{A_0,B_0}(F_0)$	$\mathbb{E}_{C_0,D_0}(G_0)$	$\mathbb{E}_{F_0,G_0}(H_0)$	$\mathbb{E}_{E_0,H_0}(I_0)$
$\mathbb{E}_{A_0,B_1}(E_1)$	$\mathbb{E}_{A_0,B_1}(F_1)$	$\mathbb{E}_{C_0,D_1}(G_1)$	$\mathbb{E}_{F_0,G_1}(H_1)$	$\mathbb{E}_{E_0,H_1}(I_1)$
$\mathbb{E}_{A_1,B_0}(E_0)$	$\mathbb{E}_{A_1,B_0}(F_1)$	$\mathbb{E}_{C_1,D_0}(G_0)$	$\mathbb{E}_{F_1,G_0}(H_0)$	$\mathbb{E}_{E_1,H_0}(I_1)$
$\mathbb{E}_{A_1,B_1}(E_0)$	$\mathbb{E}_{A_1,B_1}(F_0)$	$\mathbb{E}_{C_1,D_1}(G_0)$	$\mathbb{E}_{F_1,G_1}(H_0)$	$\mathbb{E}_{E_1,H_1}(I_1)$

Garbling a circuit:

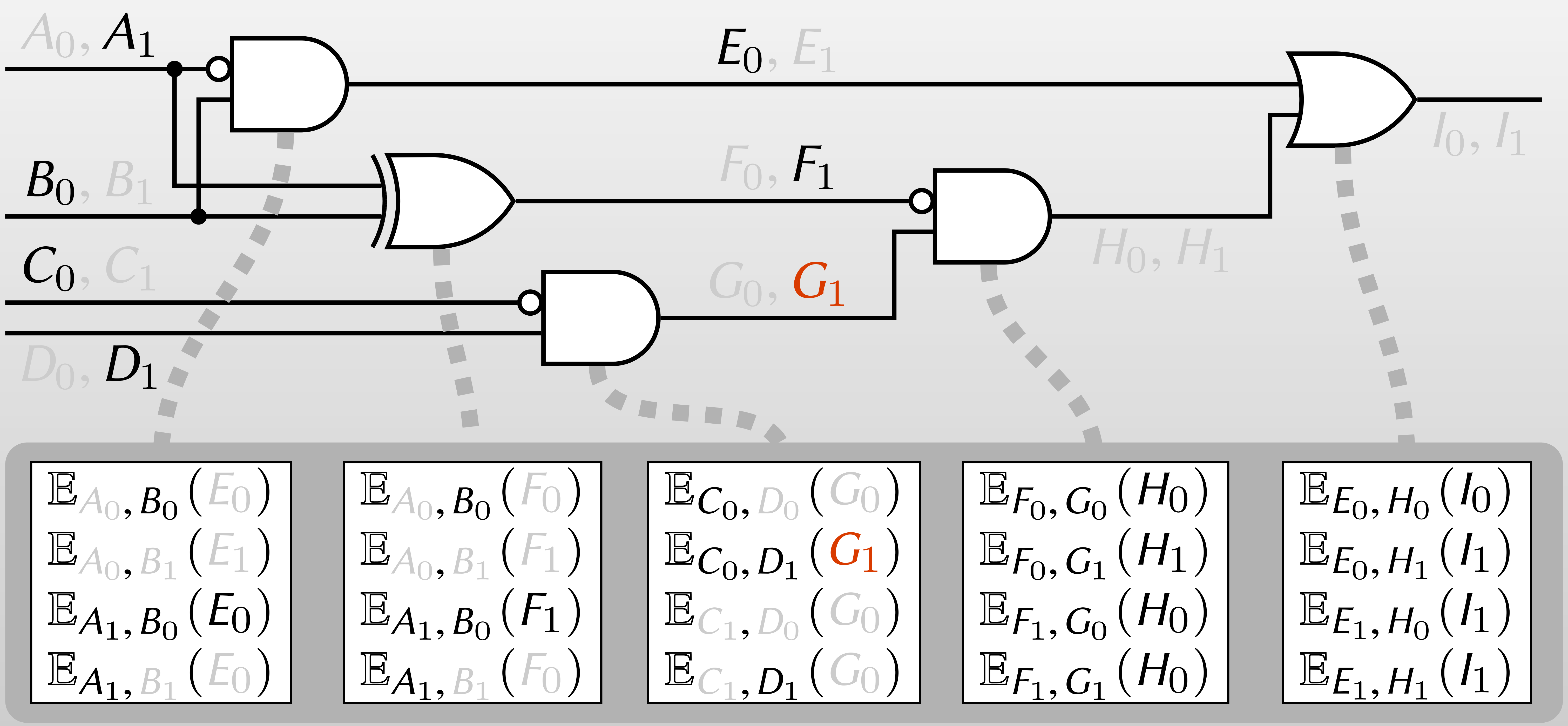
- Pick random **labels** W_0, W_1 on each wire
- "Encrypt" truth table of each gate
- **Garbled circuit** ≡ all encrypted gates
- **Garbled encoding** ≡ one label per wire

Garbled evaluation:

- Only one ciphertext per gate is decryptable
- Result of decryption = value on outgoing wire

Slides by Mike Rosulek, OSU

Garbled circuit framework [Yao86]



$\mathbb{E}_{A_0,B_0}(E_0)$	$\mathbb{E}_{A_0,B_0}(F_0)$	$\mathbb{E}_{C_0,D_0}(G_0)$	$\mathbb{E}_{F_0,G_0}(H_0)$	$\mathbb{E}_{E_0,H_0}(I_0)$
$\mathbb{E}_{A_0,B_1}(E_1)$	$\mathbb{E}_{A_0,B_1}(F_1)$	$\mathbb{E}_{C_0,D_1}(G_1)$	$\mathbb{E}_{F_0,G_1}(H_1)$	$\mathbb{E}_{E_0,H_1}(I_1)$
$\mathbb{E}_{A_1,B_0}(E_0)$	$\mathbb{E}_{A_1,B_0}(F_1)$	$\mathbb{E}_{C_1,D_0}(G_0)$	$\mathbb{E}_{F_1,G_0}(H_0)$	$\mathbb{E}_{E_1,H_0}(I_1)$
$\mathbb{E}_{A_1,B_1}(E_0)$	$\mathbb{E}_{A_1,B_1}(F_0)$	$\mathbb{E}_{C_1,D_1}(G_0)$	$\mathbb{E}_{F_1,G_1}(H_0)$	$\mathbb{E}_{E_1,H_1}(I_1)$

Garbling a circuit:

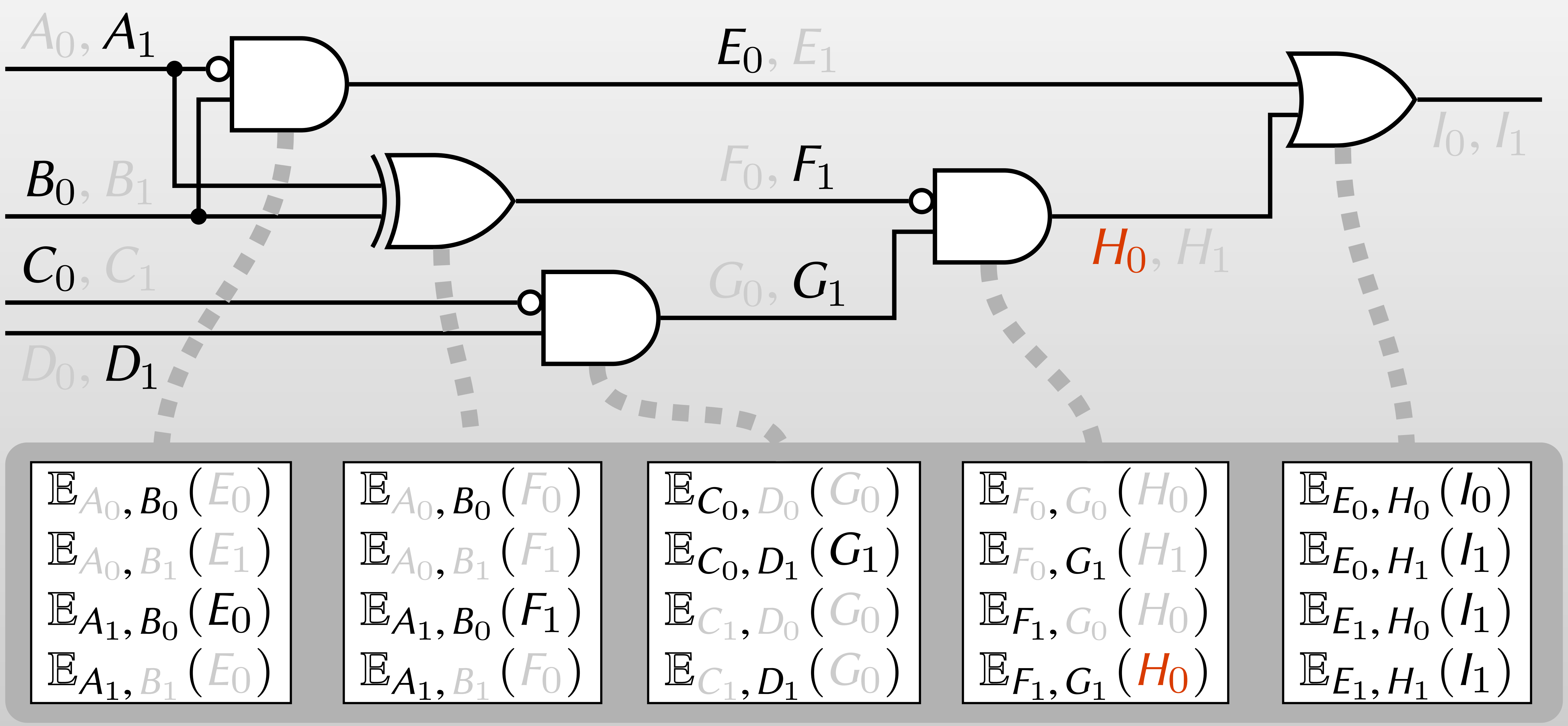
- Pick random **labels** W_0, W_1 on each wire
- “Encrypt” truth table of each gate
- **Garbled circuit** ≡ all encrypted gates
- **Garbled encoding** ≡ one label per wire

Garbled evaluation:

- Only one ciphertext per gate is decryptable
- Result of decryption = value on outgoing wire

Slides by Mike Rosulek, OSU

Garbled circuit framework [Yao86]



$\mathbb{E}_{A_0,B_0}(E_0)$	$\mathbb{E}_{A_0,B_0}(F_0)$	$\mathbb{E}_{C_0,D_0}(G_0)$	$\mathbb{E}_{F_0,G_0}(H_0)$	$\mathbb{E}_{E_0,H_0}(I_0)$
$\mathbb{E}_{A_0,B_1}(E_1)$	$\mathbb{E}_{A_0,B_1}(F_1)$	$\mathbb{E}_{C_0,D_1}(G_1)$	$\mathbb{E}_{F_0,G_1}(H_1)$	$\mathbb{E}_{E_0,H_1}(I_1)$
$\mathbb{E}_{A_1,B_0}(E_0)$	$\mathbb{E}_{A_1,B_0}(F_1)$	$\mathbb{E}_{C_1,D_0}(G_0)$	$\mathbb{E}_{F_1,G_0}(H_0)$	$\mathbb{E}_{E_1,H_0}(I_1)$
$\mathbb{E}_{A_1,B_1}(E_0)$	$\mathbb{E}_{A_1,B_1}(F_0)$	$\mathbb{E}_{C_1,D_1}(G_0)$	$\mathbb{E}_{F_1,G_1}(H_0)$	$\mathbb{E}_{E_1,H_1}(I_1)$

Garbling a circuit:

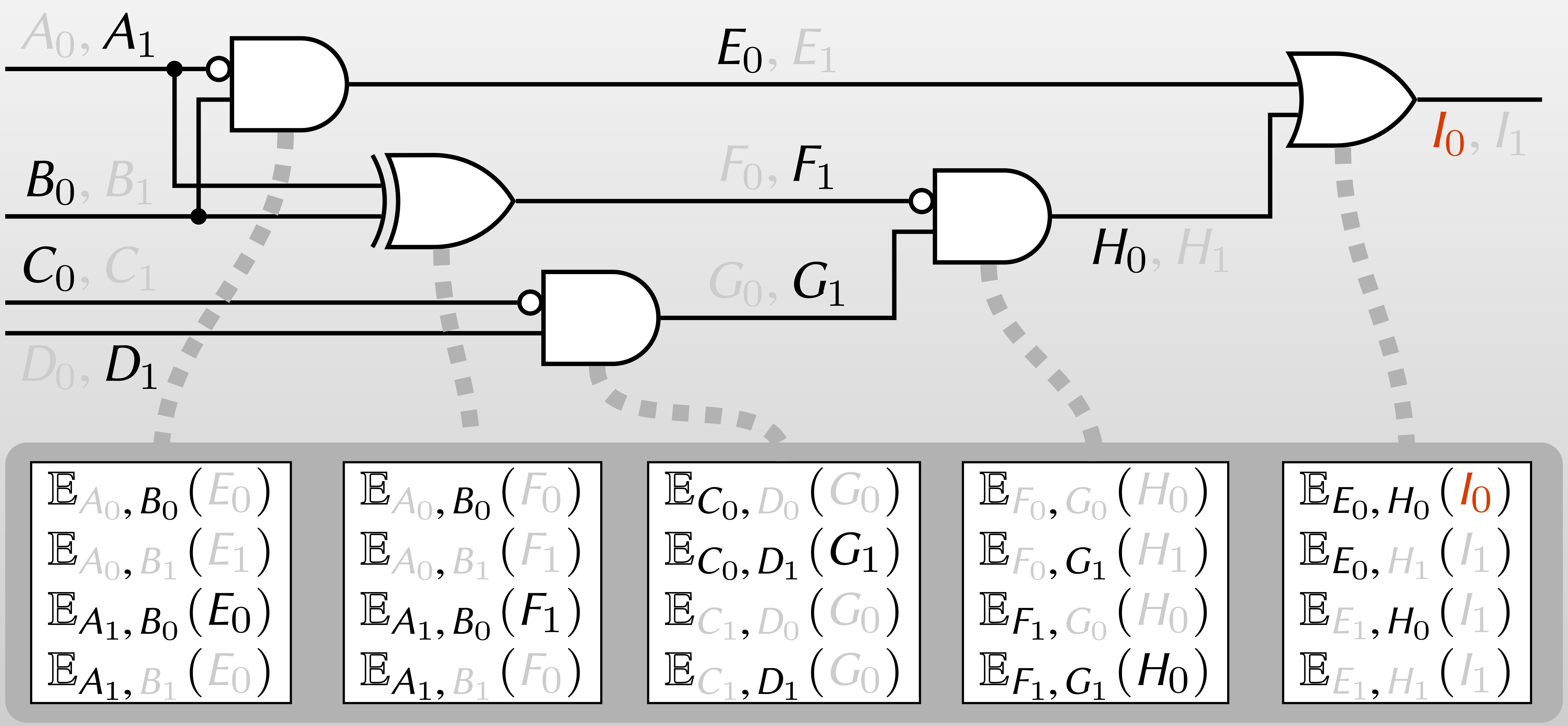
- Pick random **labels** W_0, W_1 on each wire
- “Encrypt” truth table of each gate
- **Garbled circuit** ≡ all encrypted gates
- **Garbled encoding** ≡ one label per wire

Garbled evaluation:

- Only one ciphertext per gate is decryptable
- Result of decryption = value on outgoing wire

Slides by Mike Rosulek, OSU

Garbled circuit framework [Yao86]



$\mathbb{E}_{A_0,B_0}(E_0)$	$\mathbb{E}_{A_0,B_0}(F_0)$	$\mathbb{E}_{C_0,D_0}(G_0)$	$\mathbb{E}_{F_0,G_0}(H_0)$	$\mathbb{E}_{E_0,H_0}(I_0)$
$\mathbb{E}_{A_0,B_1}(E_1)$	$\mathbb{E}_{A_0,B_1}(F_1)$	$\mathbb{E}_{C_0,D_1}(G_1)$	$\mathbb{E}_{F_0,G_1}(H_1)$	$\mathbb{E}_{E_0,H_1}(I_1)$
$\mathbb{E}_{A_1,B_0}(E_0)$	$\mathbb{E}_{A_1,B_0}(F_1)$	$\mathbb{E}_{C_1,D_0}(G_0)$	$\mathbb{E}_{F_1,G_0}(H_0)$	$\mathbb{E}_{E_1,H_0}(I_1)$
$\mathbb{E}_{A_1,B_1}(E_0)$	$\mathbb{E}_{A_1,B_1}(F_0)$	$\mathbb{E}_{C_1,D_1}(G_0)$	$\mathbb{E}_{F_1,G_1}(H_0)$	$\mathbb{E}_{E_1,H_1}(I_1)$

Garbling a circuit:

- Pick random **labels** W_0, W_1 on each wire
- “Encrypt” truth table of each gate
- **Garbled circuit** ≡ all encrypted gates
- **Garbled encoding** ≡ one label per wire

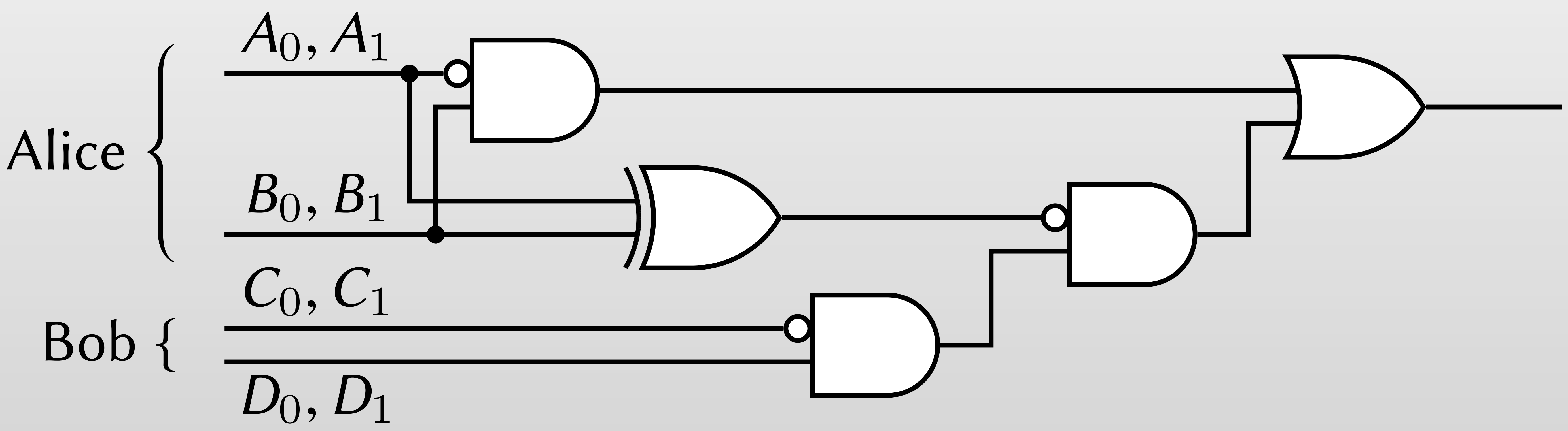
Garbled evaluation:

- Only one ciphertext per gate is decryptable
- Result of decryption = value on outgoing wire

Slides by Mike Rosulek, OSU

Oblivious transfer

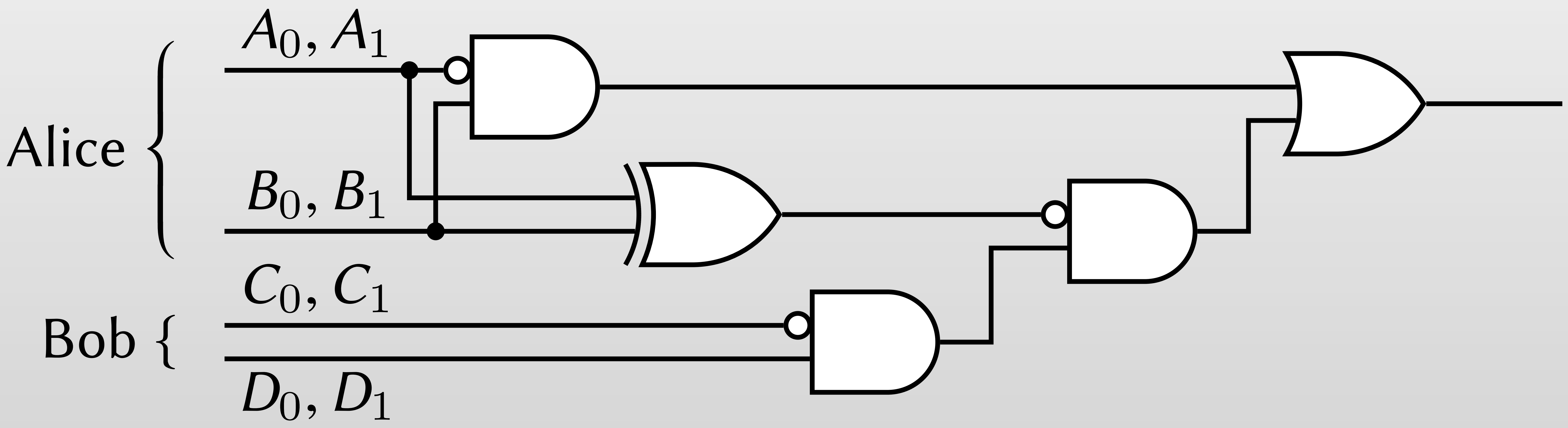
How does evaluator (Bob) get the garbled input?



Slides by Mike Rosulek, OSU

Oblivious transfer

How does evaluator (Bob) get the garbled input?

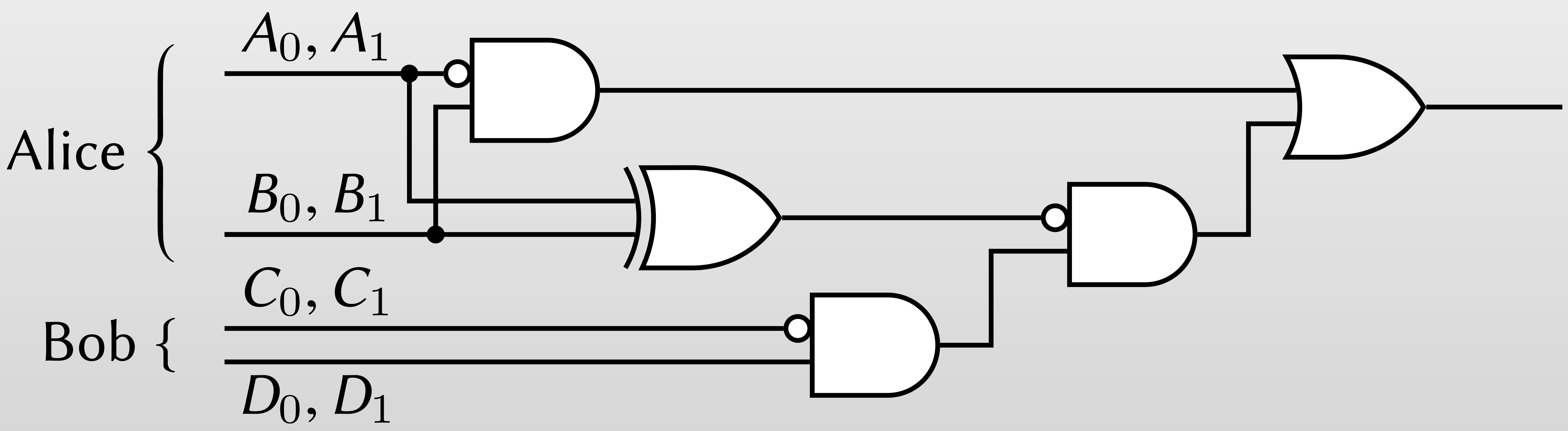


Garbler's inputs: She knows both A_0, A_1, and which one is correct ⇒ just send correct one to Bob

Slides by Mike Rosulek, OSU

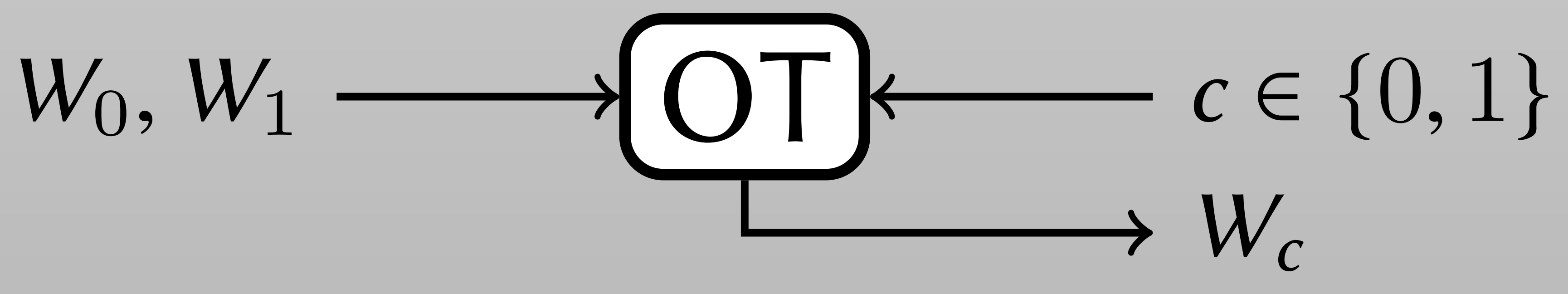
Oblivious transfer

How does evaluator (Bob) get the garbled input?



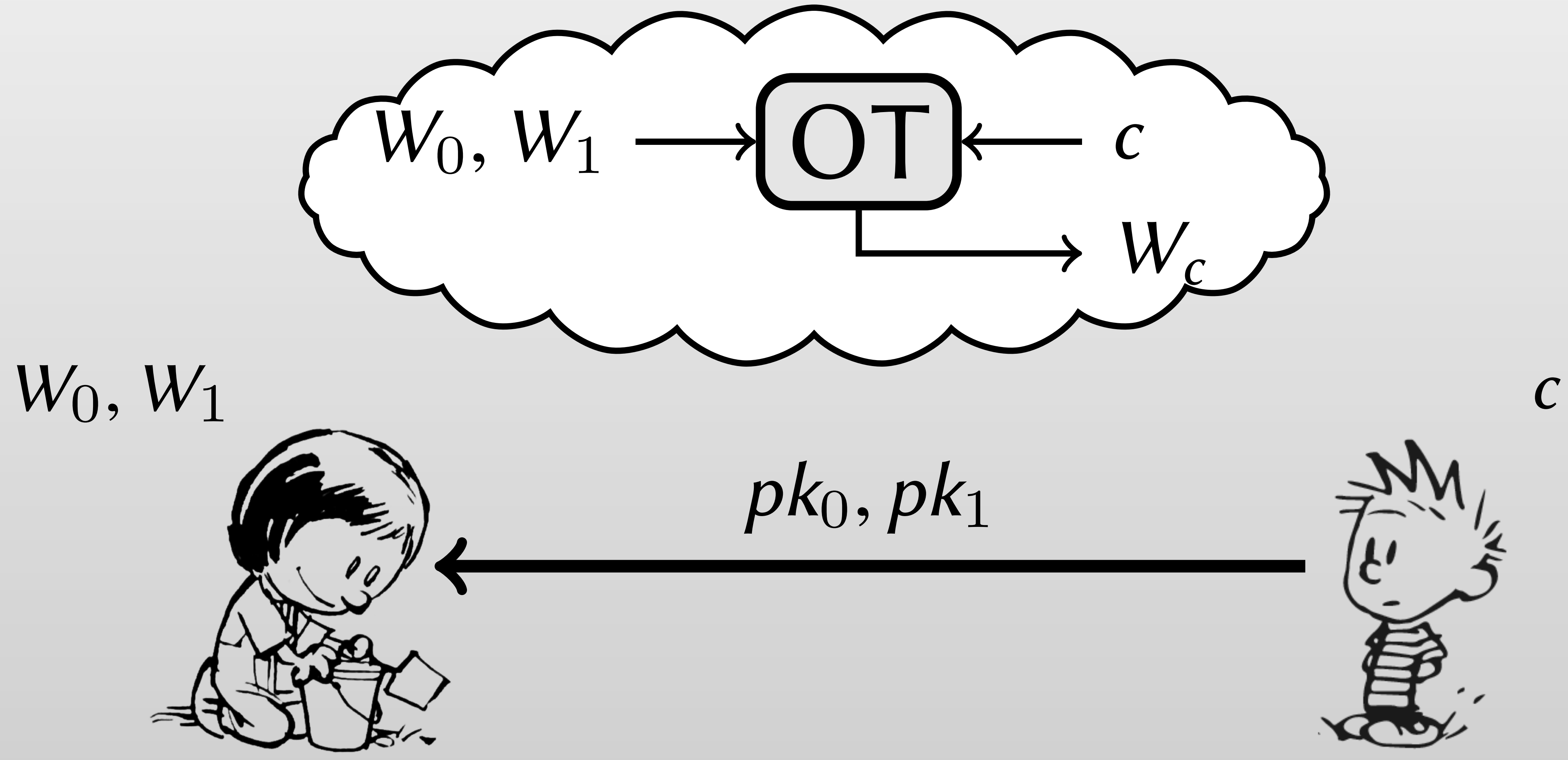
Garbler's inputs: She knows both A_0, A_1, and which one is correct $\Rightarrow$ just send correct one to Bob

Evaluator's inputs: We need the following "gadget" (oblivious transfer):



Slides by Mike Rosulek, OSU

How to construct OT?



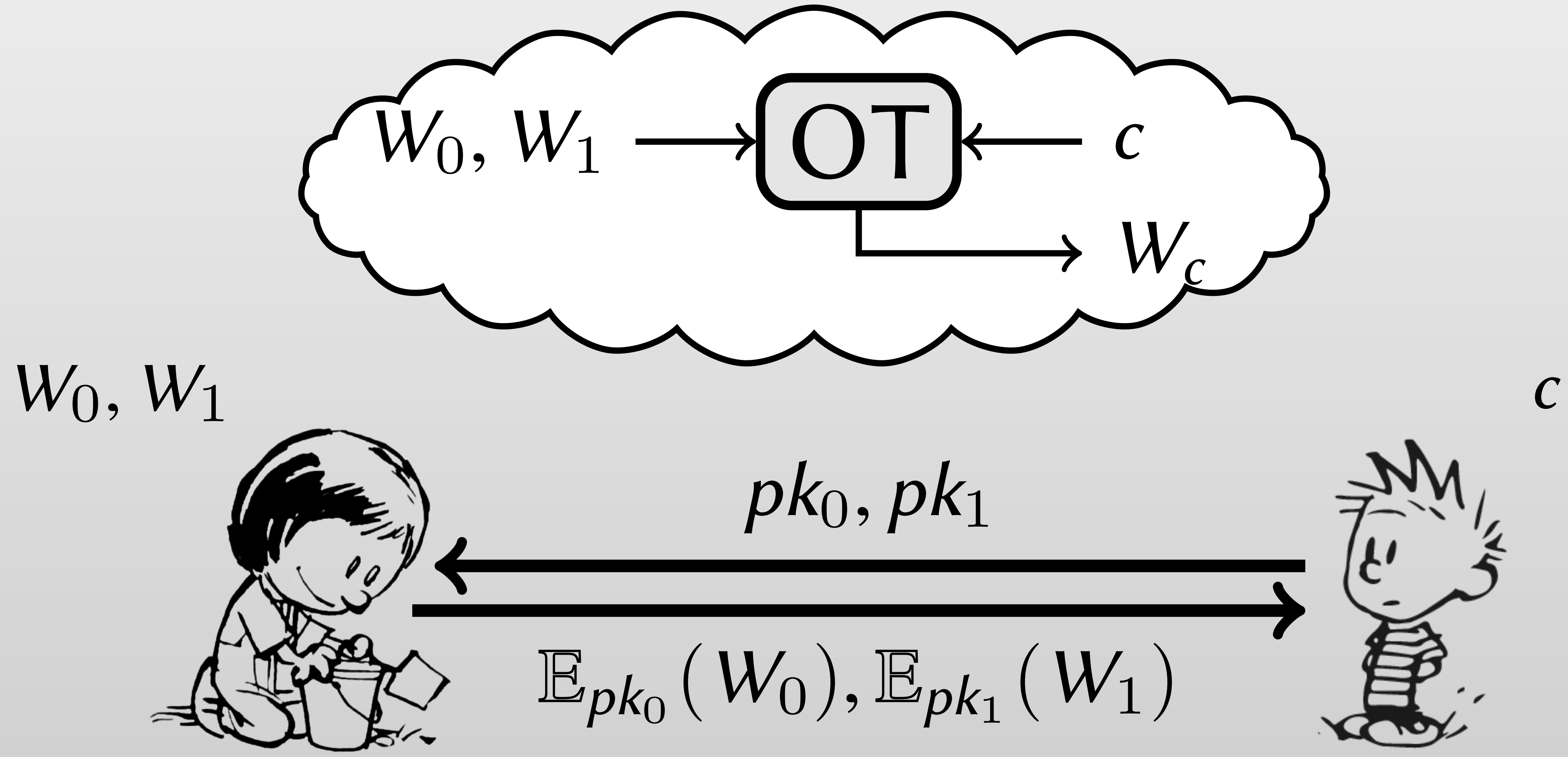
$(sk_c, pk_c) \leftarrow$ KeyGen
$pk_{1-c} \leftarrow$ BlindKeyGen

Need public-key encryption that supports **blind key generation**:

- sample a public key without knowledge of secret key
- E.g.: ElGamal (sample group element without knowing discrete log)

Slides by Mike Rosulek, OSU

How to construct OT?



$W_0, W_1 \longrightarrow \boxed{\text{OT}} \longleftarrow c$

$\boxed{\text{OT}} \longrightarrow W_c$

W_0, W_1

c

pk_0, pk_1

$\mathbb{E}_{pk_0}(W_0), \mathbb{E}_{pk_1}(W_1)$

$(sk_c, pk_c) \leftarrow \text{KeyGen}$

$pk_{1-c} \leftarrow \text{BlindKeyGen}$

Need public-key encryption that supports **blind key generation**:

- sample a public key without knowledge of secret key
- E.g.: ElGamal (sample group element without knowing discrete log)

Slides by Mike Rosulek, OSU

Summary so far

Secure Computation allows parties to perform a computation on private input, learning only the output.

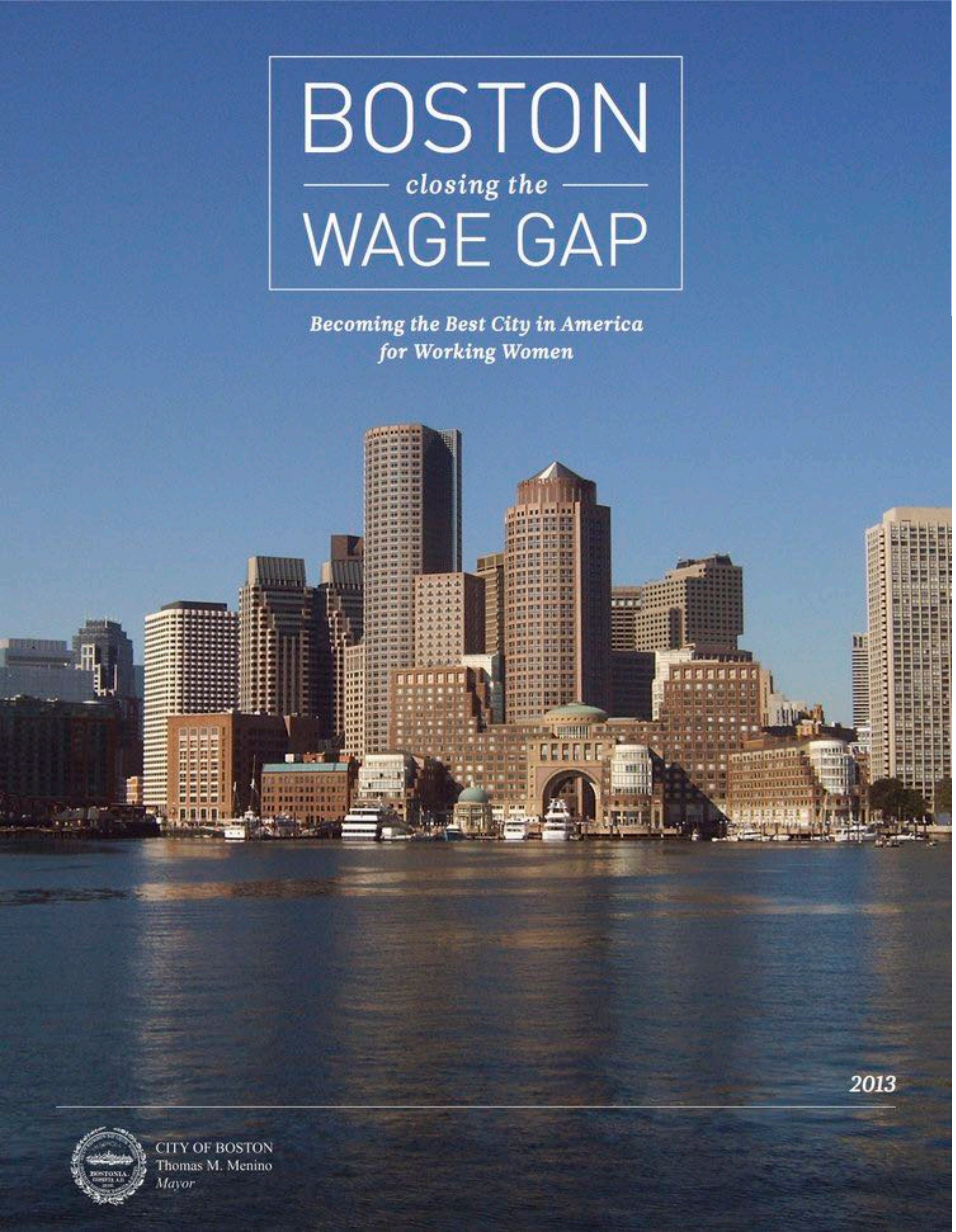
- market clearing price, advertising revenue, . . .

Security: every attack against the protocol can be “simulated” in an ideal world interaction.

Yao’s protocol:

- Garbled lookup table for each gate of boolean circuit
- Oblivious transfer for each input wire

Slides by Mike Rosulek, OSU



BOSTON
closing the
WAGE GAP

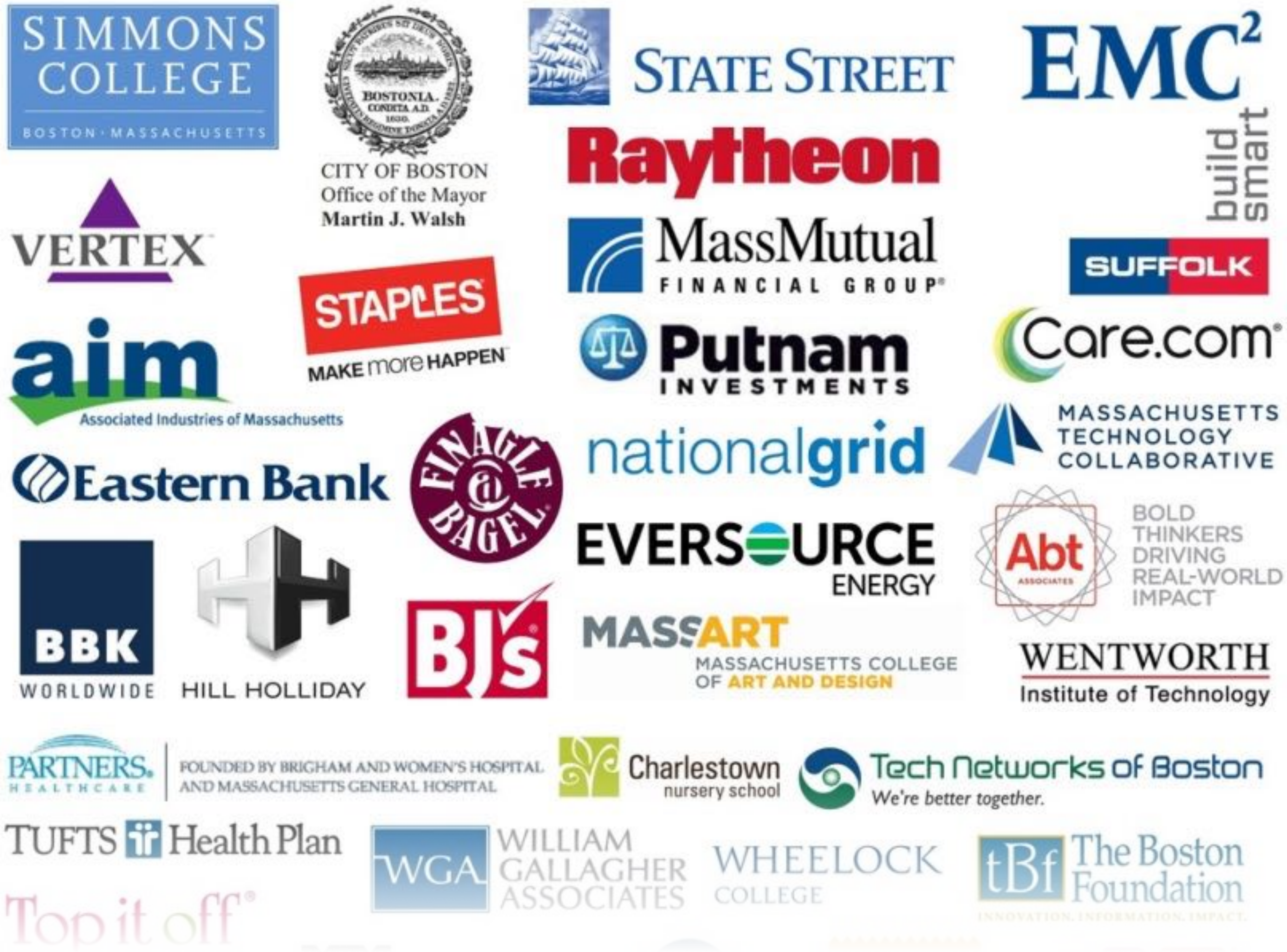
Becoming the Best City in America for Working Women

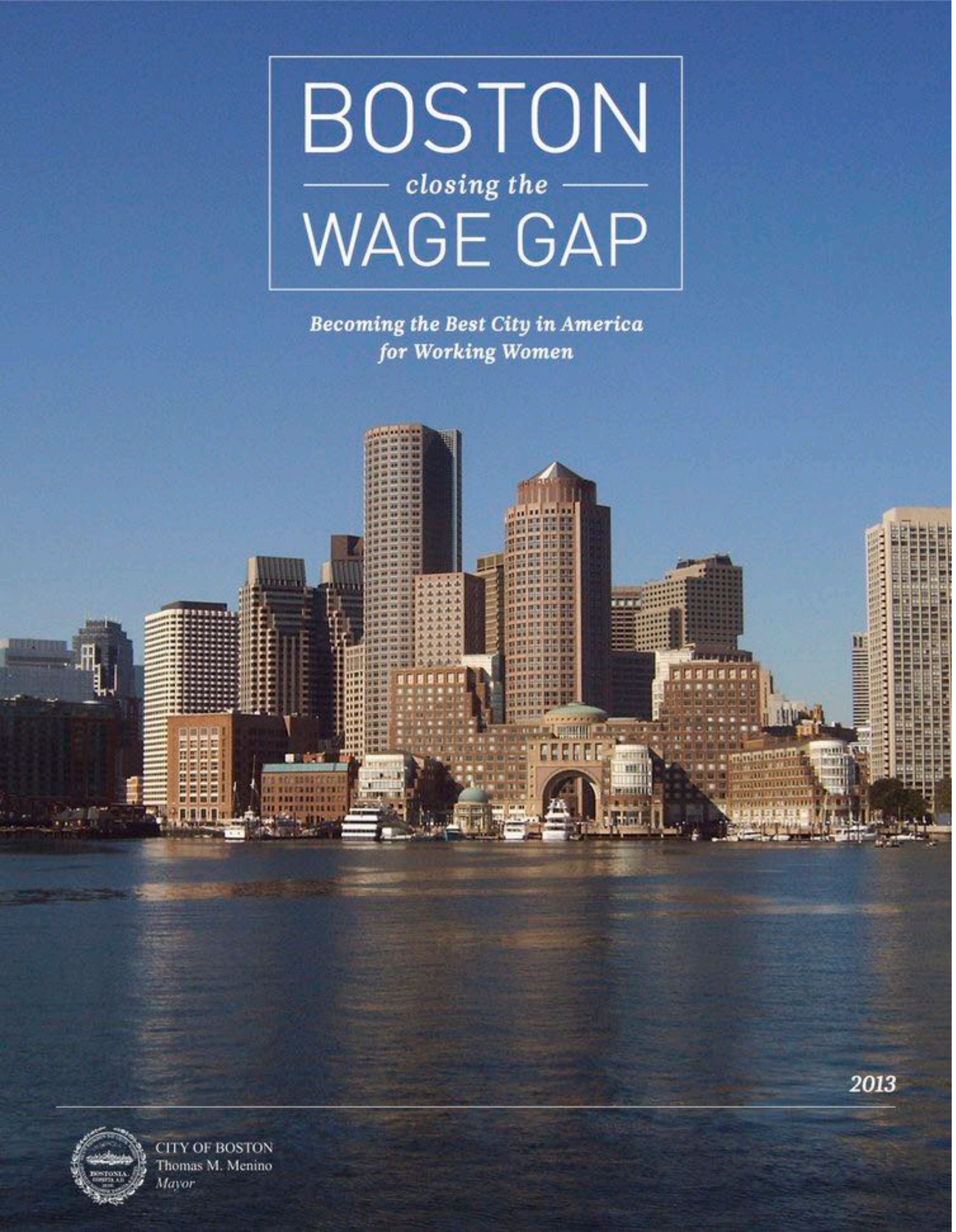
2013

CITY OF BOSTON
Thomas M. Menino
Mayor

100% TALENT

The Boston Women's Compact


SIMMONS COLLEGE BOSTON · MASSACHUSETTS
CITY OF BOSTON Office of the Mayor Martin J. Walsh
STATE STREET
EMC²
Raytheon
build smart
VERTEX
MassMutual FINANCIAL GROUP
SUFFOLK
STAPLES MAKE more HAPPEN
aim Associated Industries of Massachusetts
Putnam INVESTMENTS
Care.com
nationalgrid
MASSACHUSETTS TECHNOLOGY COLLABORATIVE
Eastern Bank
FINAGLE A BAGEL
EVERSOURCE ENERGY
Abt ASSOCIATES
BOLD THINKERS DRIVING REAL-WORLD IMPACT
BBK WORLDWIDE
HILL HOLLIDAY
BJ's
MASSART MASSACHUSETTS COLLEGE OF ART AND DESIGN
WENTWORTH Institute of Technology
PARTNERS. HEALTHCARE FOUNDED BY BRIGHAM AND WOMEN'S HOSPITAL AND MASSACHUSETTS GENERAL HOSPITAL
Charlestown nursery school
Tech Networks of Boston We're better together.
TUFTS Health Plan
WGA WILLIAM GALLAGHER ASSOCIATES
WHEELOCK COLLEGE
tBf The Boston Foundation INNOVATION. INFORMATION. IMPACT.
Top it off



BOSTON

closing the

WAGE GAP

Becoming the Best City in America for Working Women

2013

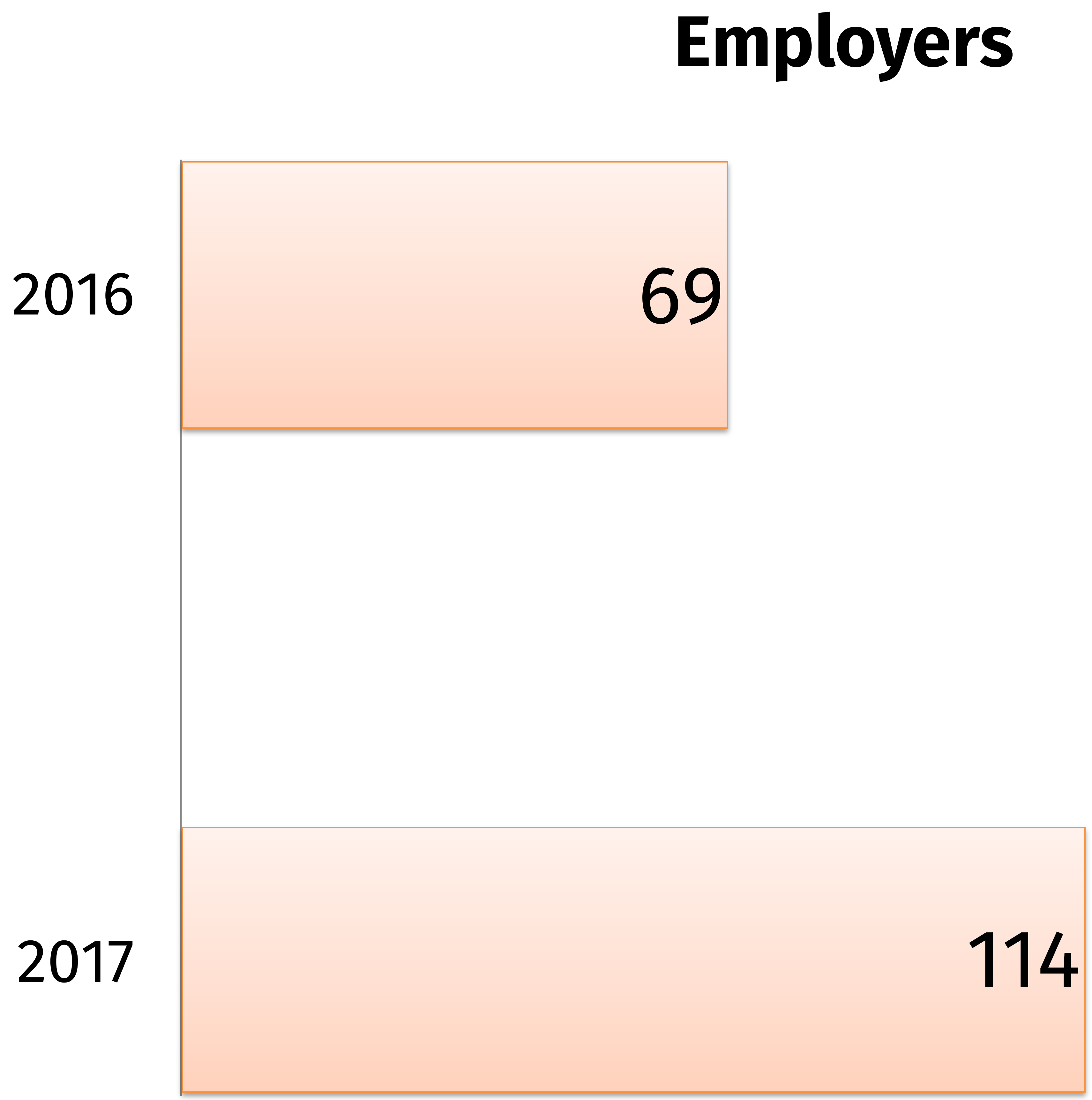
CITY OF BOSTON
Thomas M. Menino
Mayor

100% TALENT

The Boston Women's Compact

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.



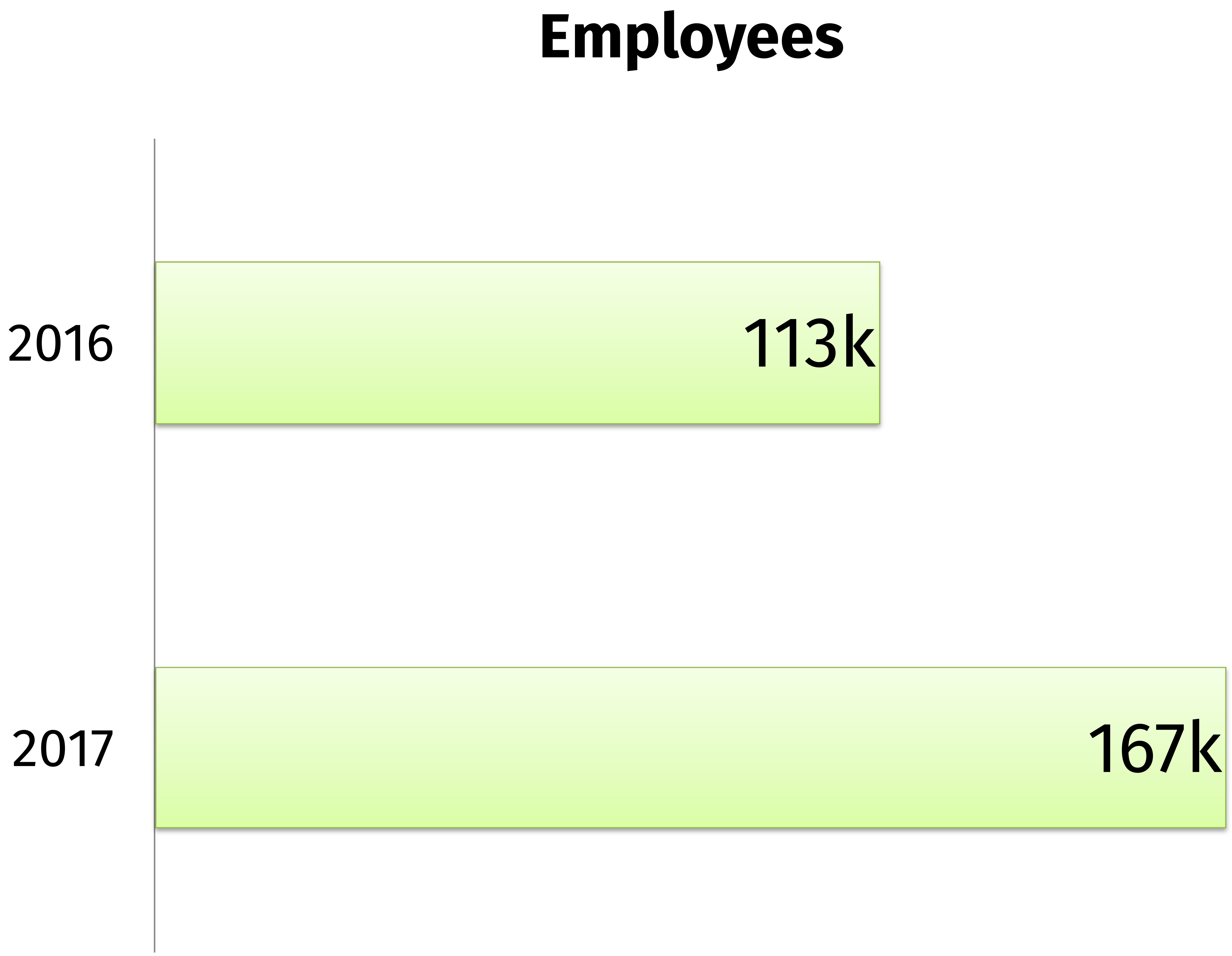


Image: Wikipedia

Boston Women's Workforce Co
Secure
https://100talent.org
BOSTON UNIVERSITY
100% TALENT

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 Co
Secure https://100talent.org
100% TALENT
BOSTON UNIVERSITY

Boston Women's Workforce Council

100% Talent Data Submission

Number Of Employees

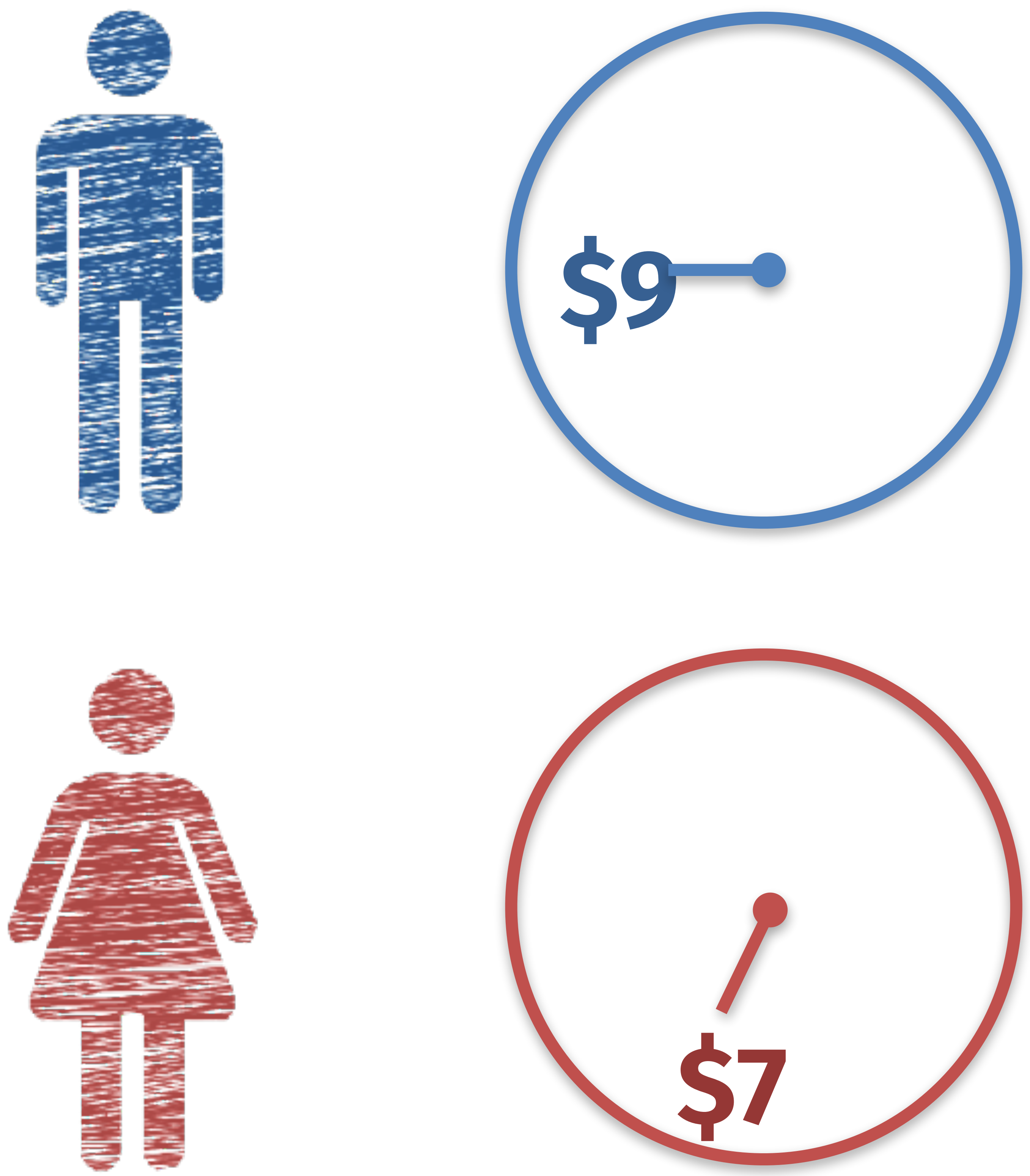
	Hispanic or Latinx		White		Black/African American		Native Hawaiian or Pacific Islander		Asian		American Indian/Alaska Native		Two or More Races (Not Hispanic or Latinx)		Unreported	
	Female	Male	Female	Male	Female	Male	Female	Male	Female	Male	Female	Male	Female	Male	Female	Male
Executive/Senior Level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

Total Annual Compensation (Dollars)

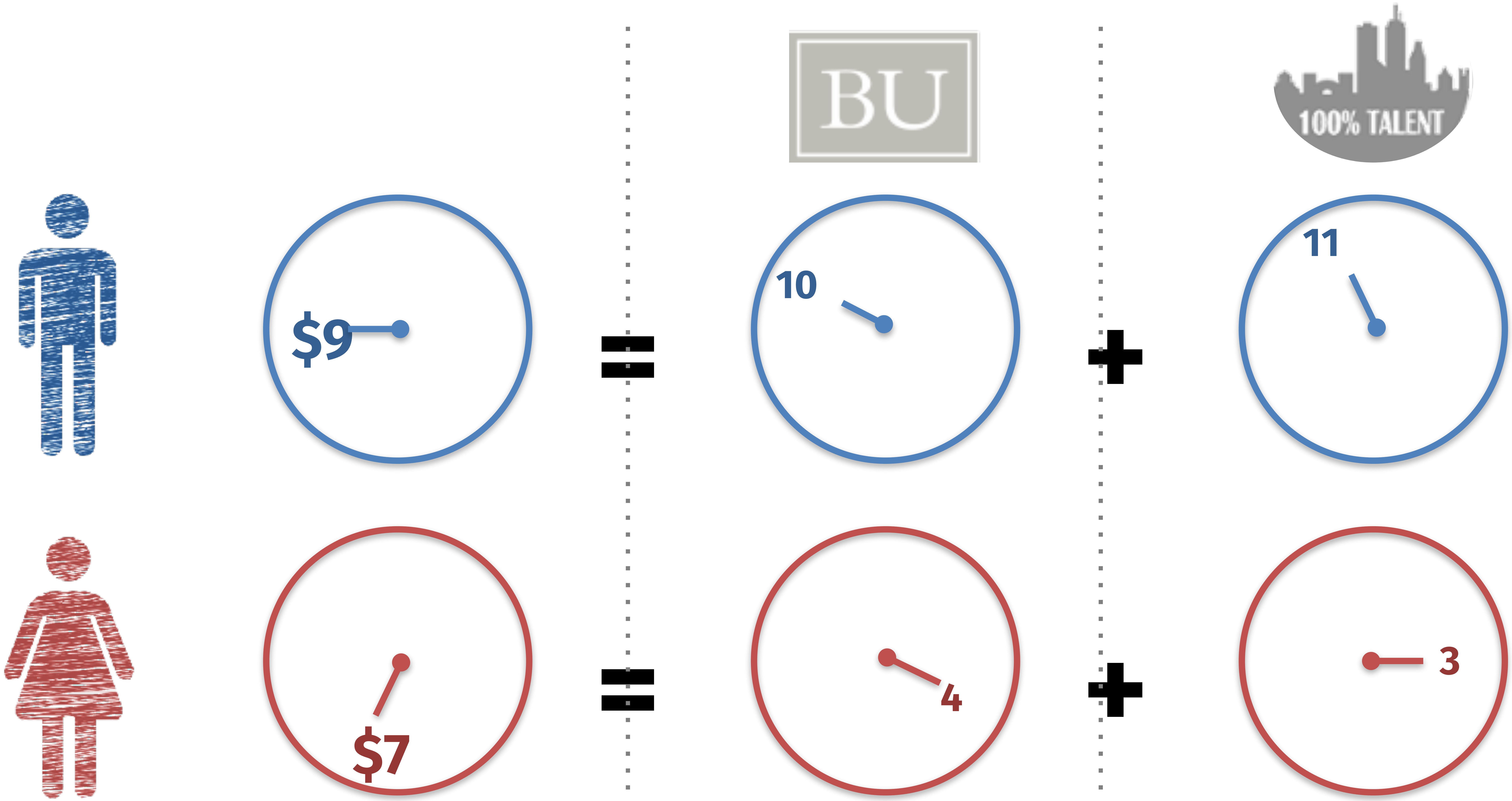
	Hispanic or Latinx		White		Black/African American		Native Hawaiian or Pacific Islander		Asian		American Indian/Alaska Native		Two or More Races (Not Hispanic or Latinx)		Unreported	
	Female	Male	Female	Male	Female	Male	Female	Male	Female	Male	Female	Male	Female	Male	Female	Male
Executive/Senior Level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

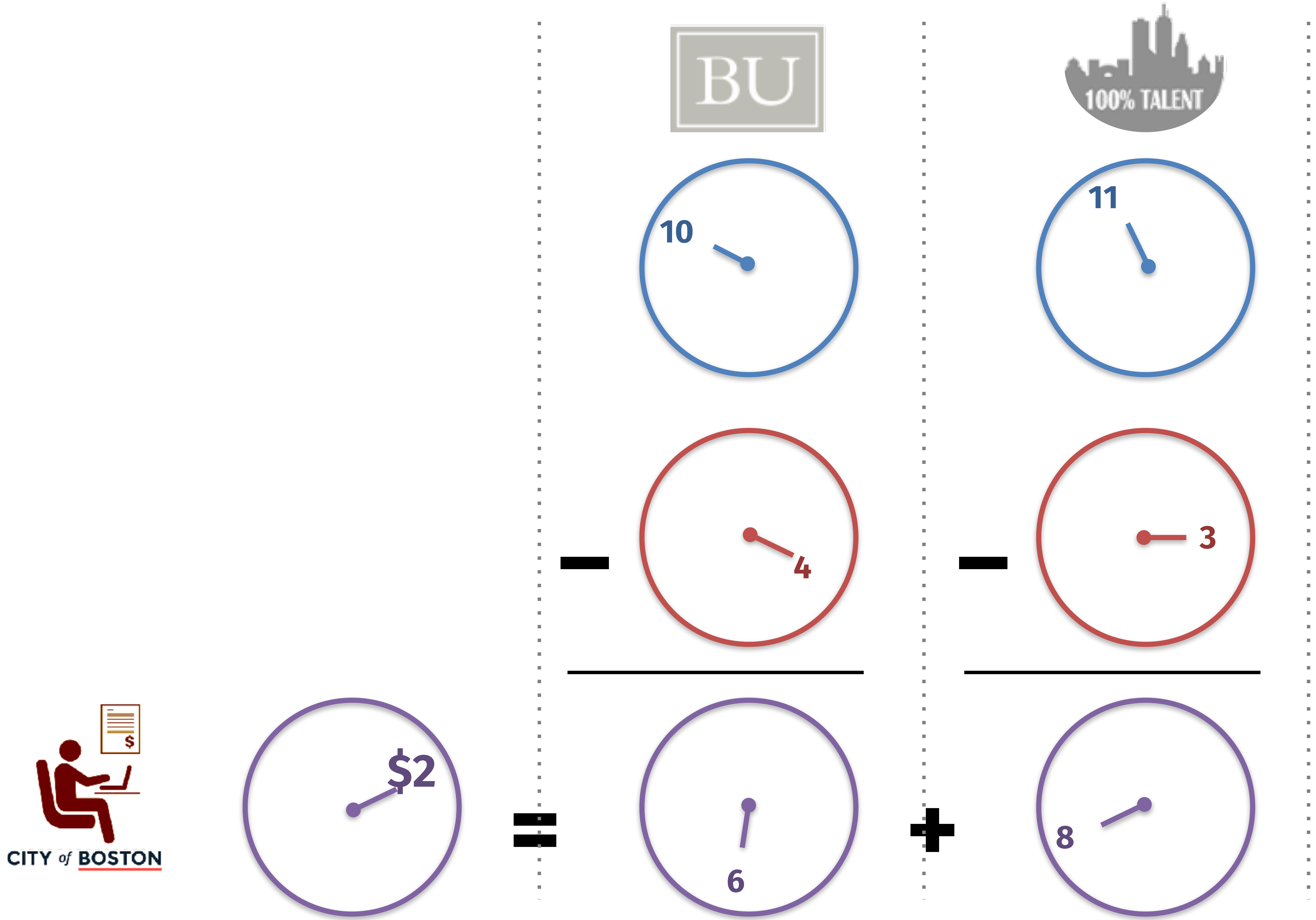
BU

100% TALENT



CITY of BOSTON


BU
100% TALENT
$9
10
11
$7
4
3


BU
100% TALENT
10
11
–
4
–
3
CITY of BOSTON
$2
=
6
+
8

Trust Spectrum

Trust us

Trust anyone

Trust no one

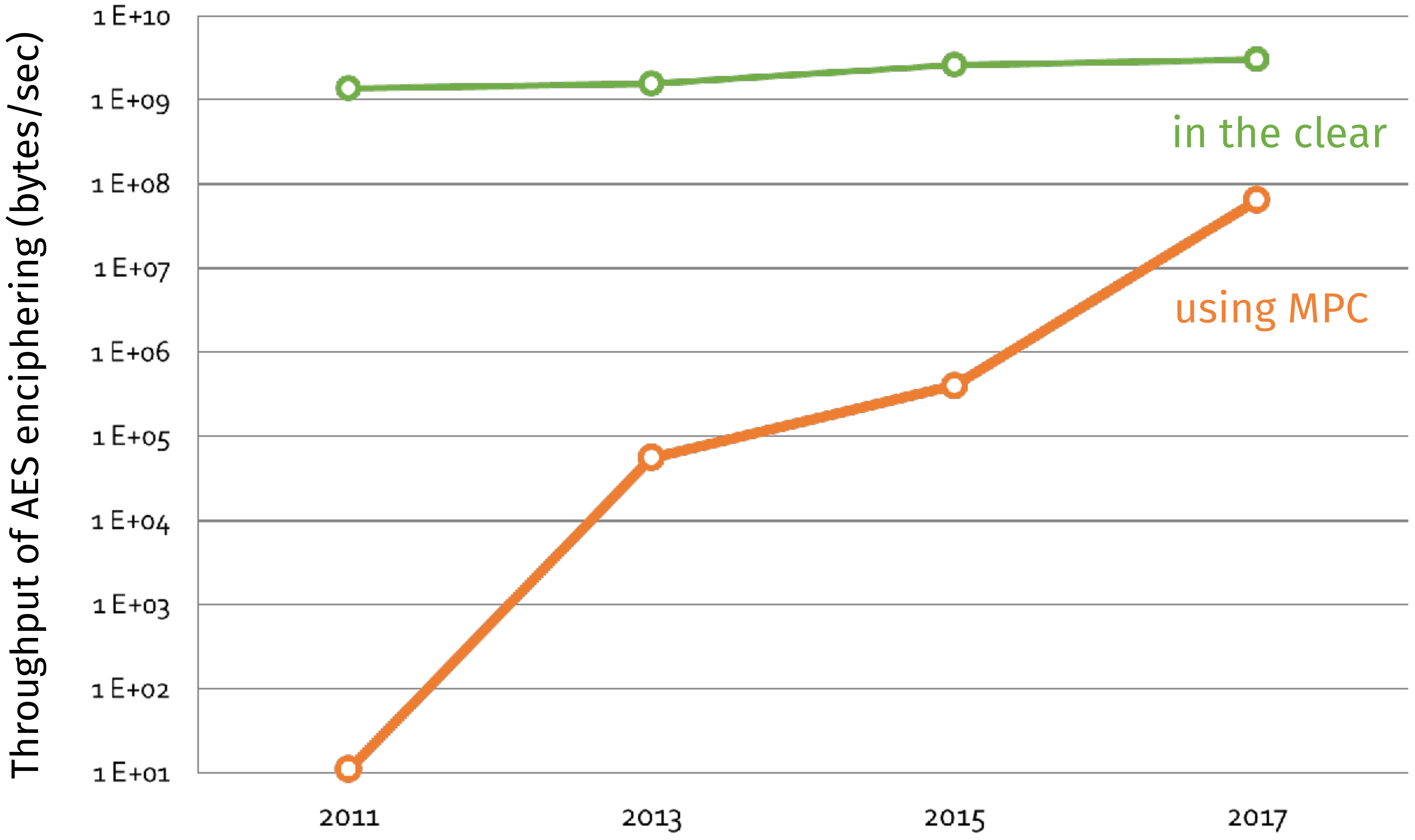
BU

BOSTON WOMEN'S WORKFORCE COUNCIL

100% TALENT

Techniques for cryptographically secure computing

- Garbled circuits
- Secret sharing



Additional applications of protected computing

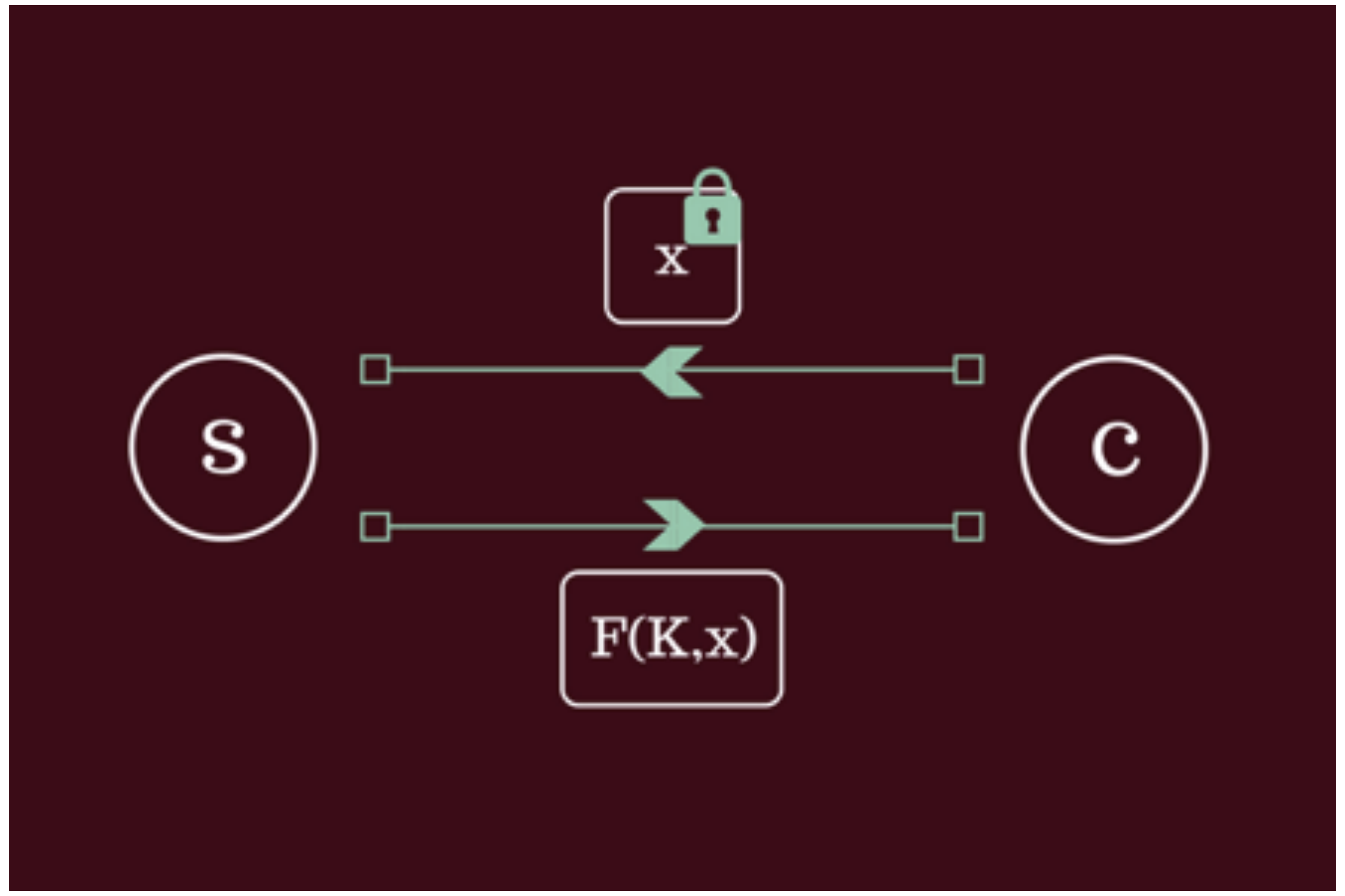
Cloudflare: anonymous web browsing

Image: Wikipedia

Please type the two words below to ensure that a person, not an automated program, is submitting this form.*

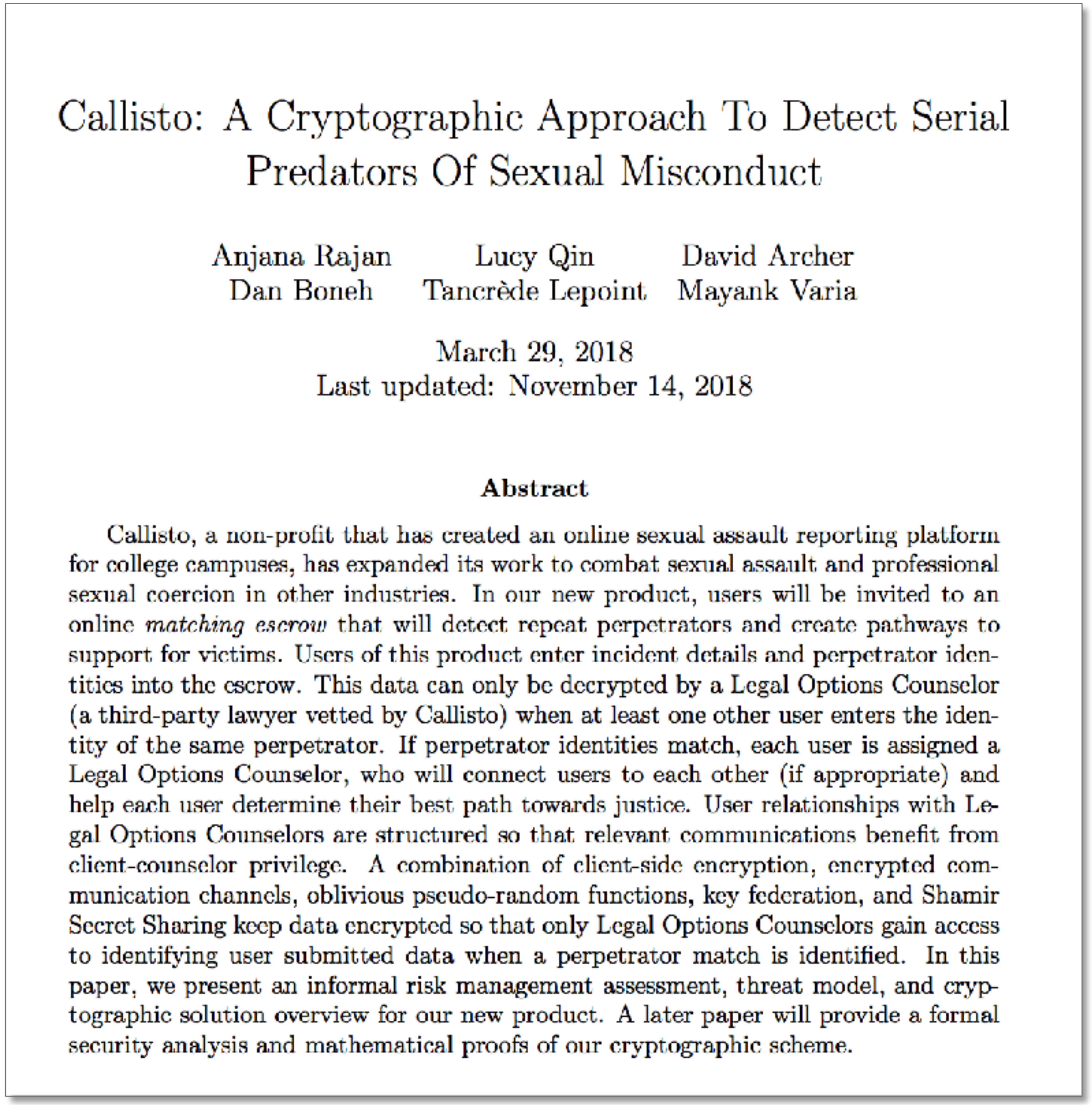
Type the two words:

- Goal: anonymous authentication
- Primitive: verifiable oblivious PRF



Source: Davidson, Goldberg, Sullivan, Tankersley, and Valsorda, *Privacy Pass: Bypassing Internet Challenges Anonymously*

BU + CALLISTO



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

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

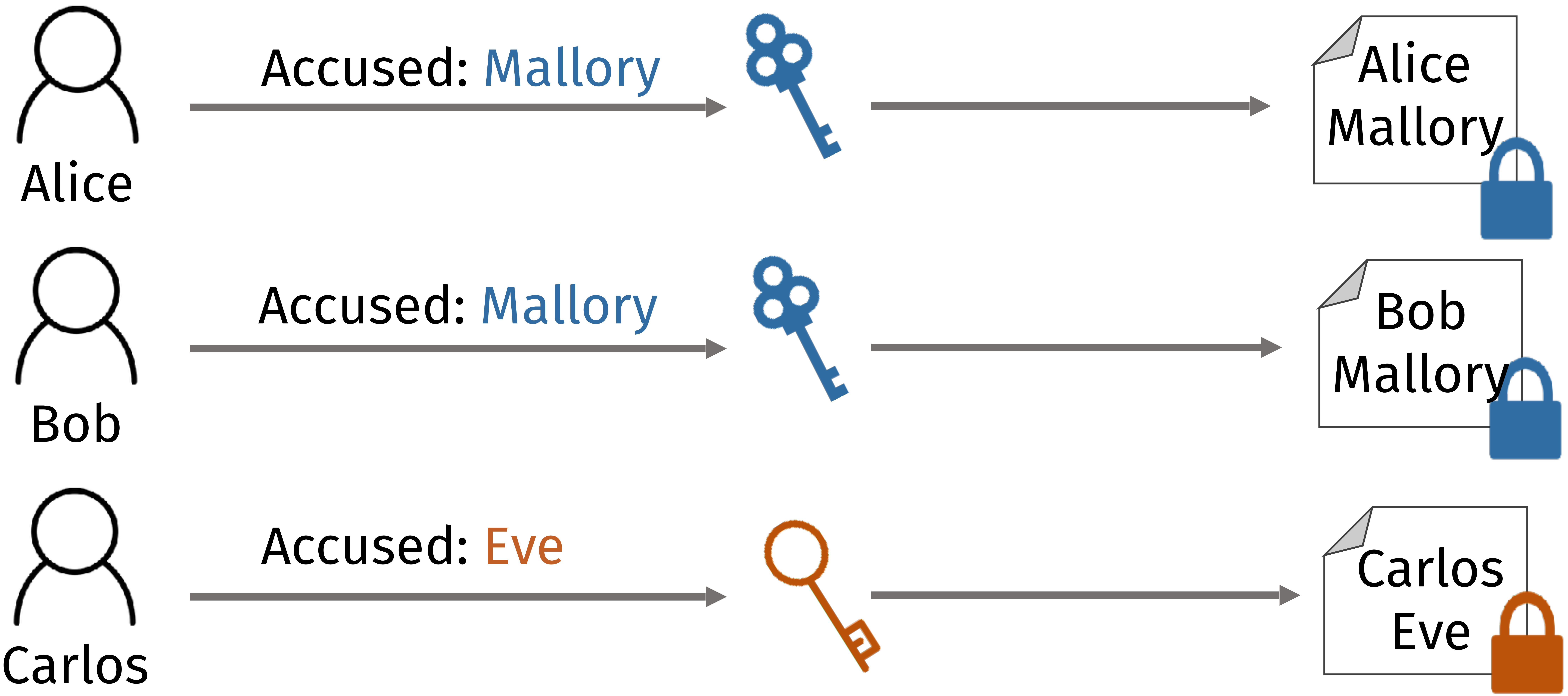
March 29, 2018
Last updated: November 14, 2018

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.

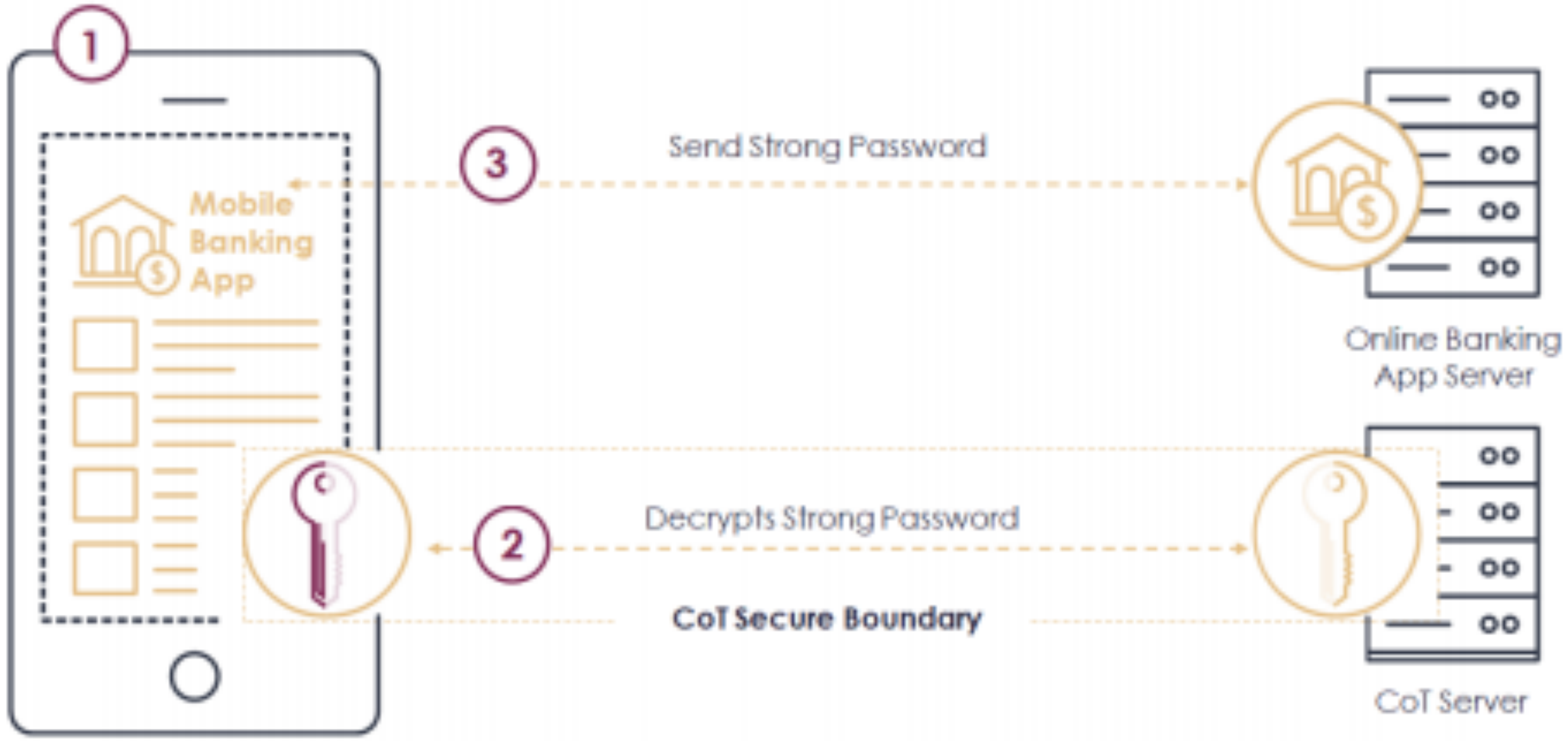
- Identifying information about a survivor and the accused can only be decrypted by a lawyer when at least 2 users name the same perpetrator
- Demo available online at cryptography.projectcallisto.org

BU + CALLISTO


Alice
Accused: Mallory
Alice
Mallory
Bob
Accused: Mallory
Bob
Mallory
Carlos
Accused: Eve
Carlos
Eve

Protecting cryptographic keys

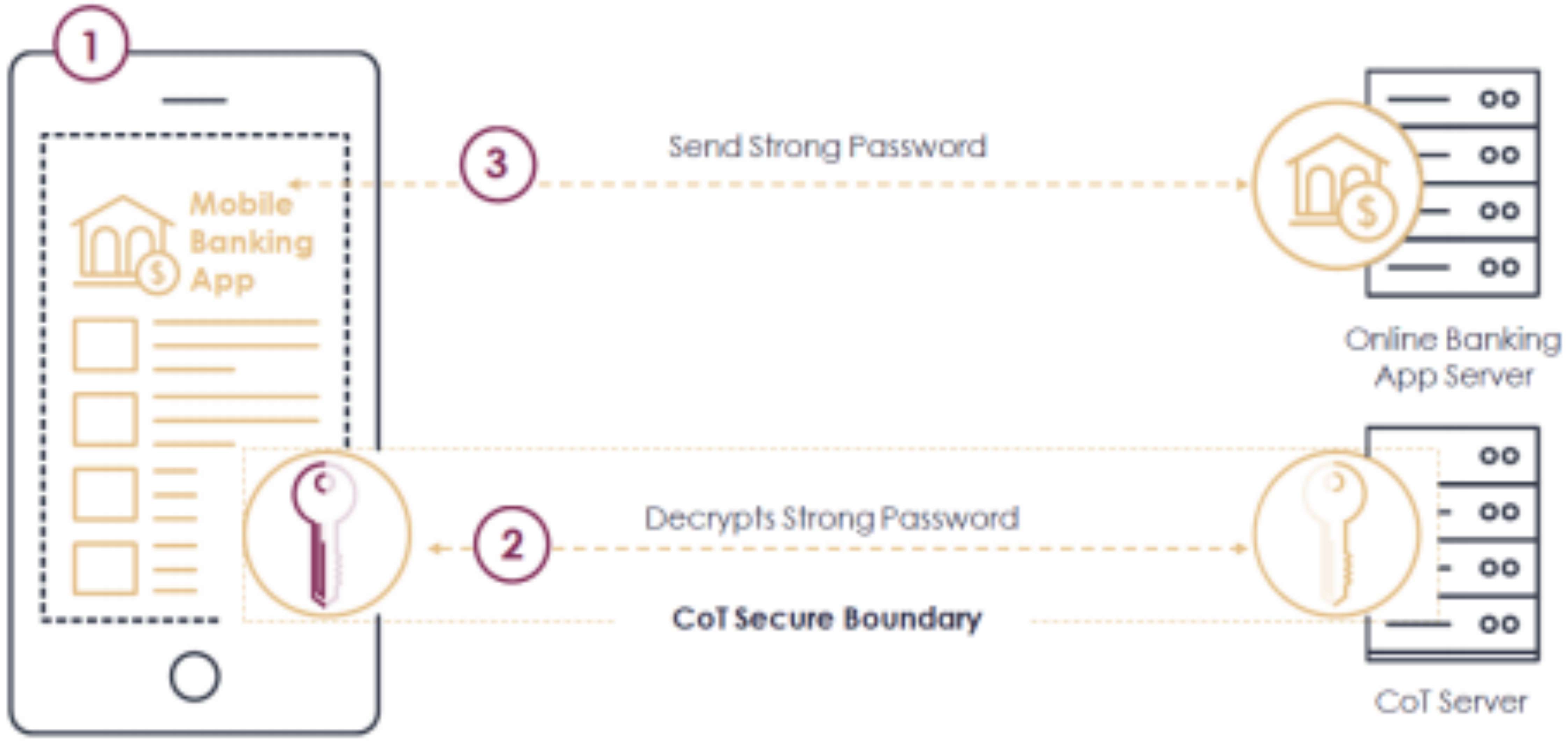
Unbound tech



Source: Archer et al, *From Keys to Databases – Real-World Applications of Secure MPC*

Protecting cryptographic keys

Unbound tech



Source: Archer et al, *From Keys to Databases – Real-World Applications of Secure MPC*

Preveil

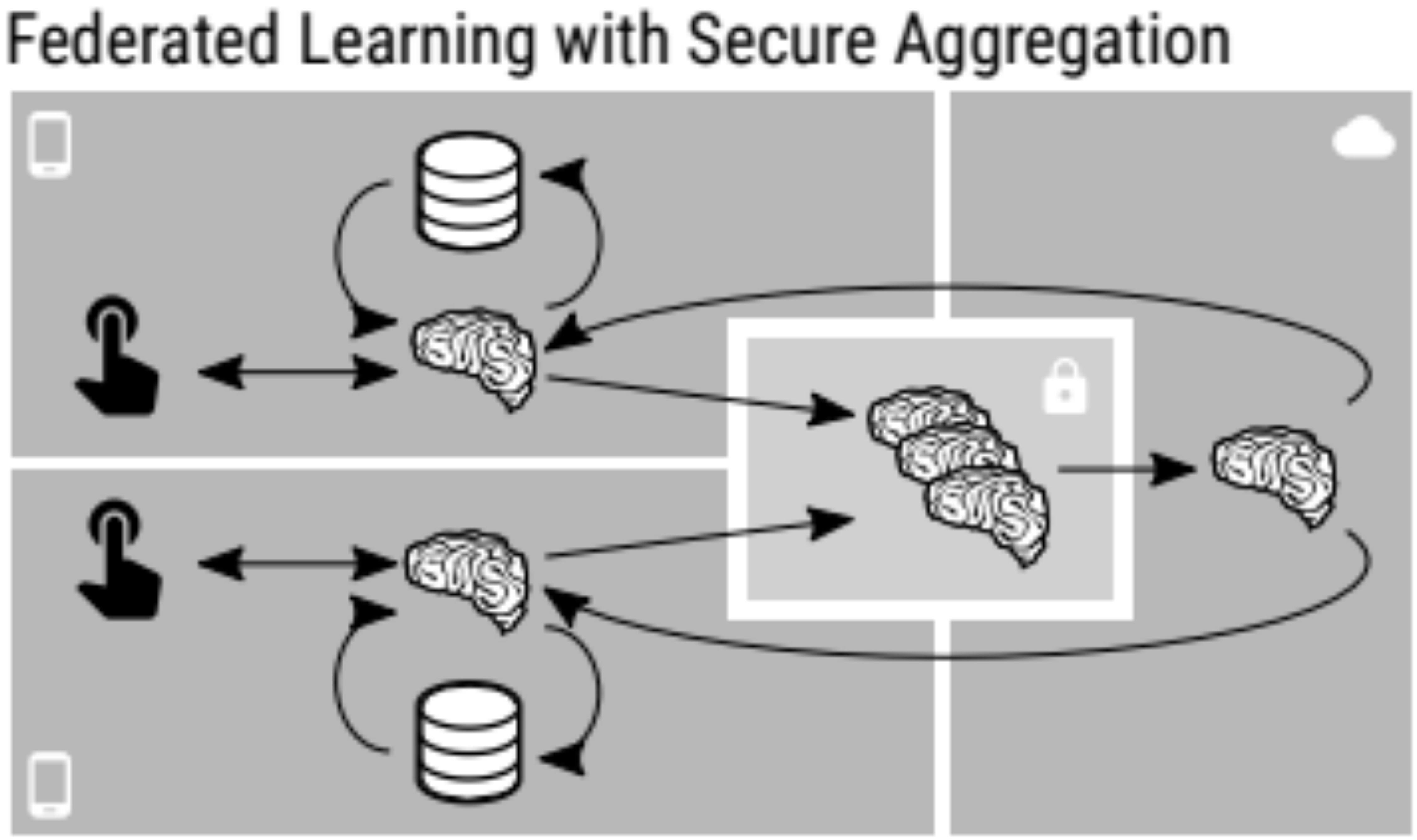
"IT can still access encrypted corporate information and recover user keys using Approval Groups. They are the cryptographic equivalent of giving fragments of your house key to your neighbors. No single neighbor can access your house, but if you lose your key, your neighbors can get you back in."

Source: www.preveil.com

Google: keyboard predictions

- Train a deep neural network for keyboard typing predictions

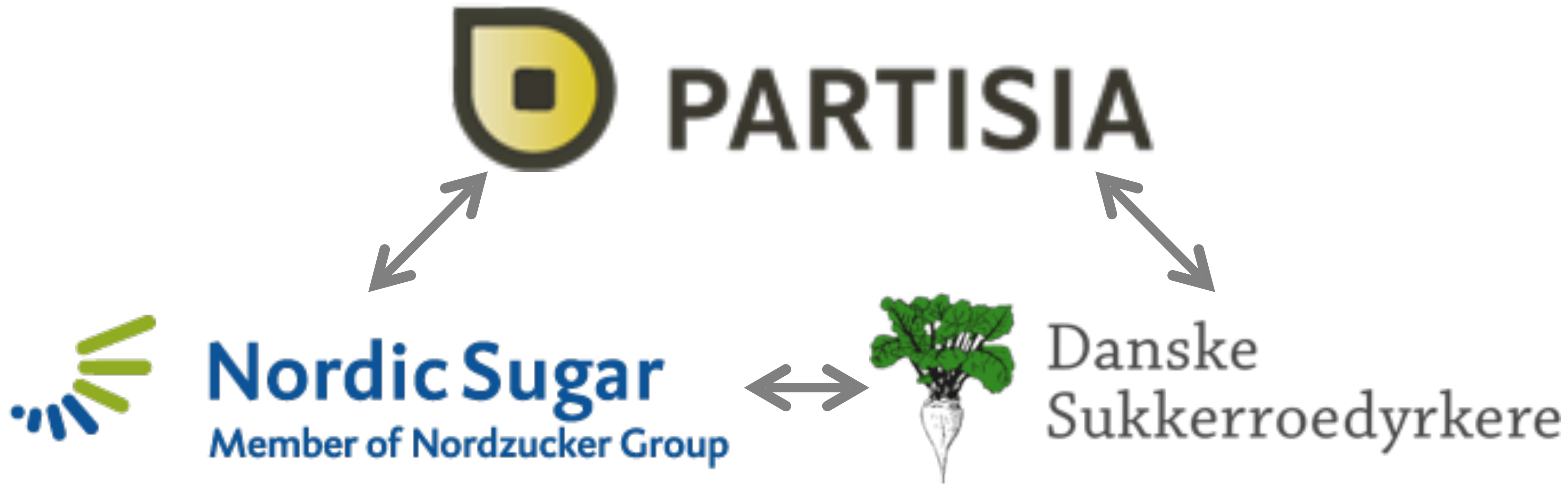
- Stochastic gradient descent over high-dimensional vectors



Source: Bonawitz, Ivanov, Kreuter, Marcedone, McMahan, Patel, Ramage, Segal, and Seth, *Practical Secure Aggregation for Privacy-Preserving Machine Learning*

Partisia: financial markets

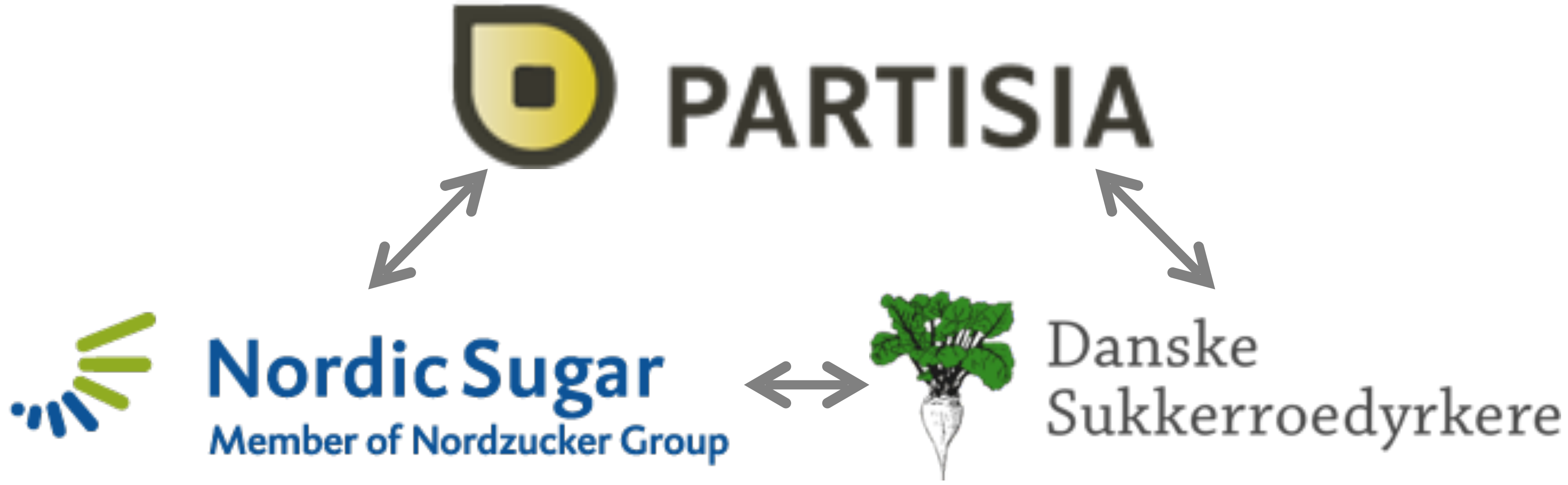
- Auctions (eg sugar beets)



Source: Bogetoft, Christensen, Damgard, Geisler, Jakobsen, Krøigaard, Nielsen, Nielsen, Nielsen, Pagter, Schwartzbach, and Toft, *Secure Multiparty Computation Goes Live*

Partisia: financial markets

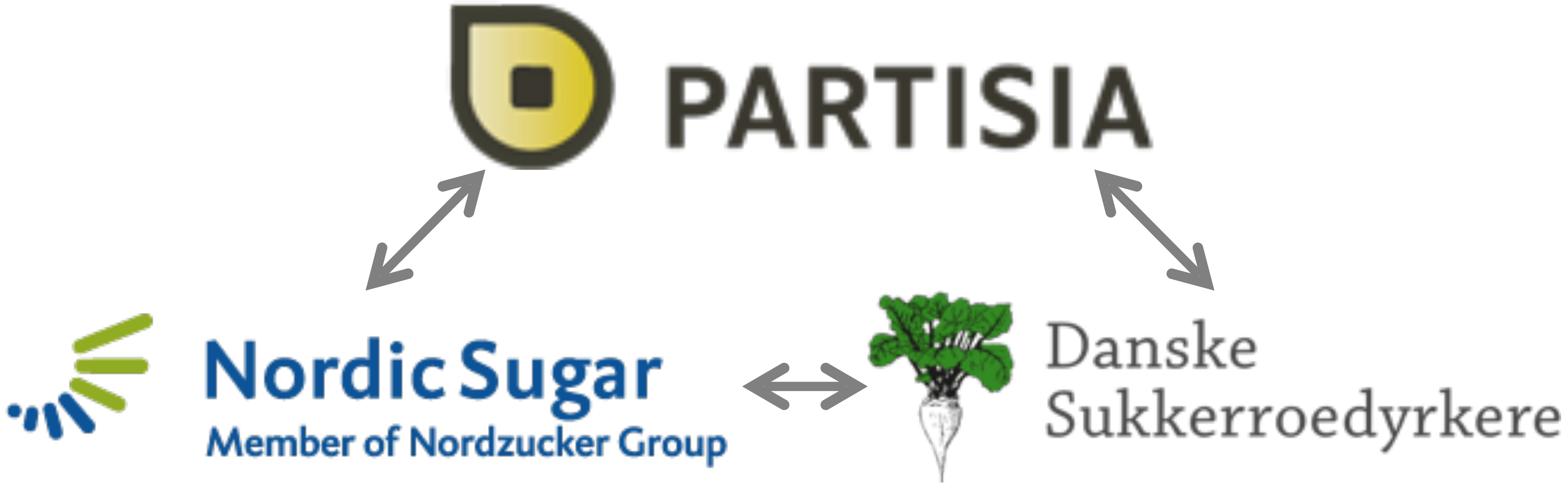
- Auctions (eg sugar beets)
- Market clearinghouse
  - Match incoming orders
  - Compare with price signals from realized trades



Source: Archer, Bogdanov, Lindell, Kamm, Nielsen, Pagter, Smart, and Wright,
From Keys to Databases – Real-World Applications of Secure MPC

Partisia: financial markets

- Auctions (eg sugar beets)
- Market clearinghouse
  - Match incoming orders
  - Compare with price signals from realized trades
- Credit rating
  - Uses linear programming
  - Input: farmers of all banks

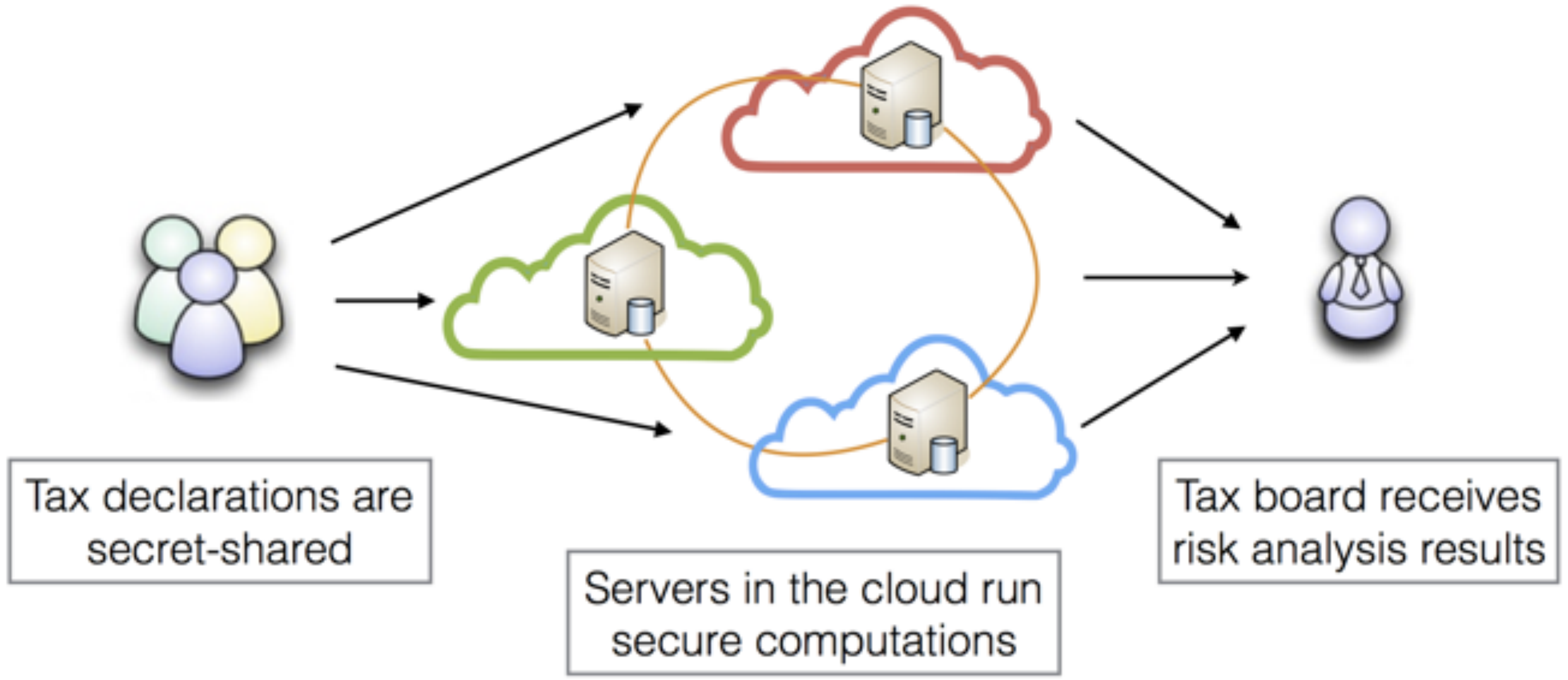


Source: Damgard, Damgard, Nielsen, Nordholt, and Toft, *Confidential Benchmarking based on Multiparty Computation*

Sharemind: audit VAT tax revenue

- Worked with Estonian Tax and Customs Board

- Test if Company A’s VAT credit == Company B’s VAT reported



Tax declarations are secret-shared

Servers in the cloud run secure computations

Tax board receives risk analysis results

Source: https://sharemind.cyber.ee/tax-vat-fraud/

Sharemind: education outcomes

Questions

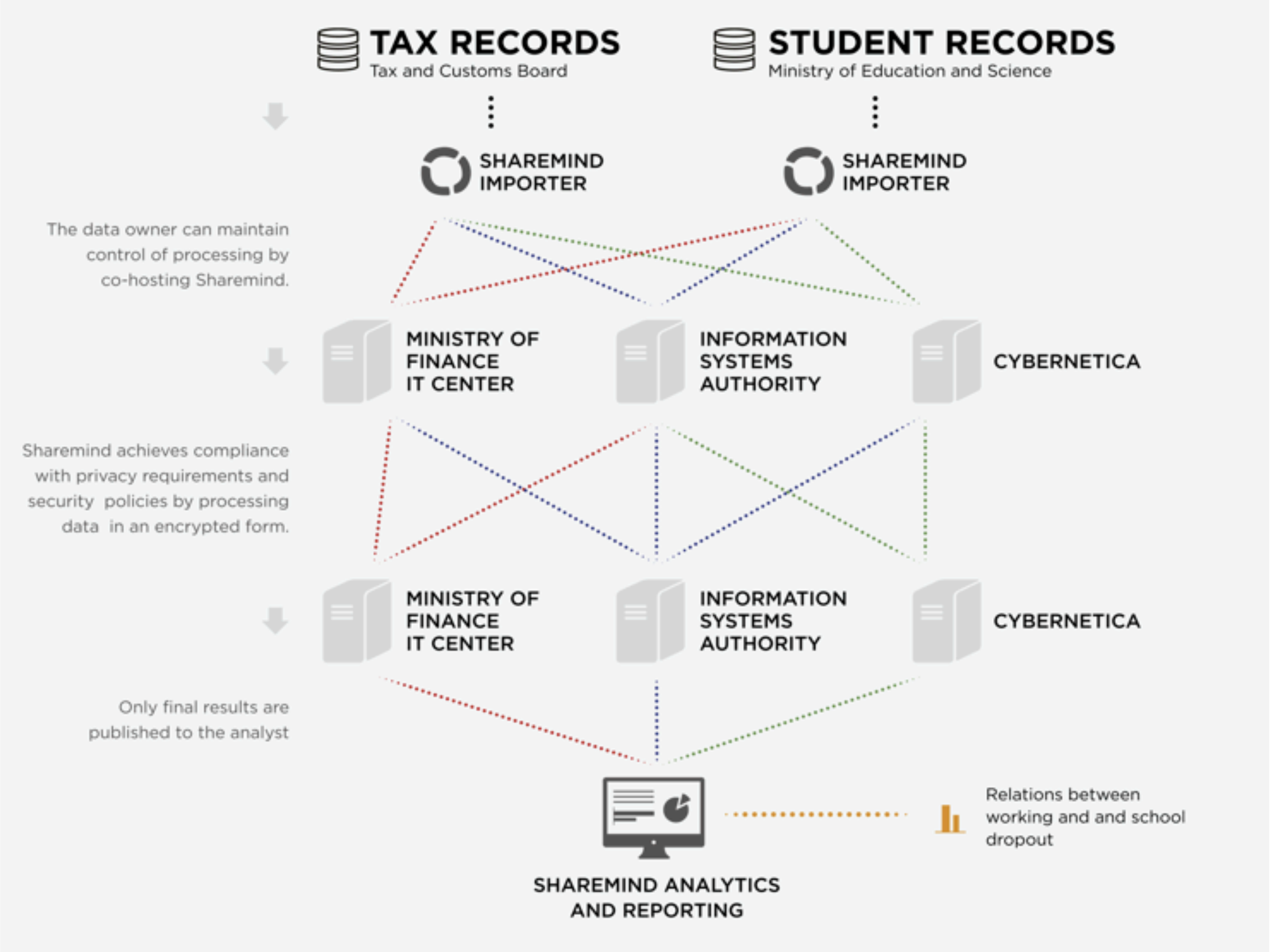
- Effect of work on graduation rate?
- Diff between CS & other students?

Data size

- 600k education records
- 10m tax payment records

Performance

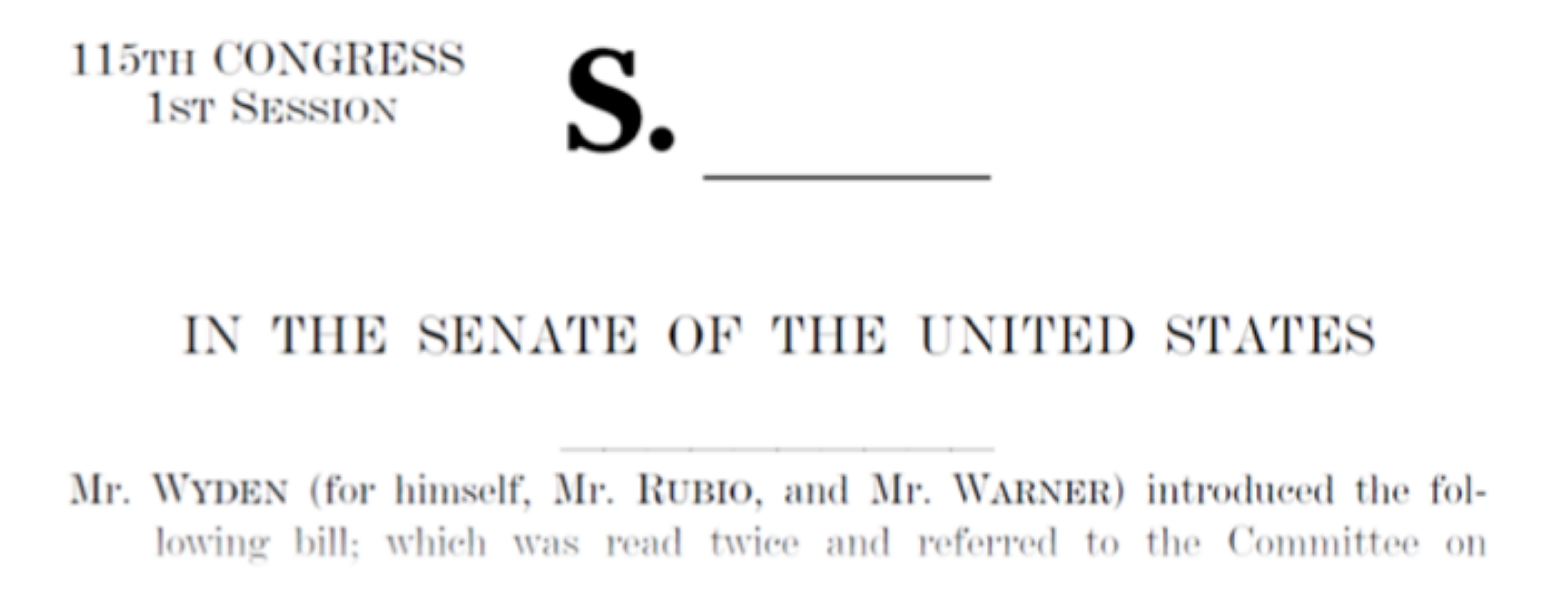
- 384.5 hours during live study
- 5 hours after optimizations


TAX RECORDS
Tax and Customs Board
STUDENT RECORDS
Ministry of Education and Science
SHAREMIND IMPORTER
SHAREMIND IMPORTER
The data owner can maintain control of processing by co-hosting Sharemind.
MINISTRY OF FINANCE IT CENTER
INFORMATION SYSTEMS AUTHORITY
CYBERNETICA
Sharemind achieves compliance with privacy requirements and security policies by processing data in an encrypted form.
MINISTRY OF FINANCE IT CENTER
INFORMATION SYSTEMS AUTHORITY
CYBERNETICA
Only final results are published to the analyst
Relations between working and and school dropout
SHAREMIND ANALYTICS AND REPORTING

Source: Bogdanov, Kamm, Kubo, Rebane, Sokk, and Talviste,
Students and Taxes: a Privacy-Preserving Social Study Using Secure Computation

US education outcomes: coming soon?

- College Transparency Act
- Student Right to Know Before You Go



115TH CONGRESS
1ST SESSION

S. ____

IN THE SENATE OF THE UNITED STATES

Mr. WYDEN (for himself, Mr. RUBIO, and Mr. WARNER) introduced the following bill; which was read twice and referred to the Committee on

“in designing, establishing, and maintaining the higher education data system, ... the Commissioner shall use ***secure multiparty computation technologies***”