Web-based Multi-Party Computation

with Application to Anonymous Aggregate Compensation Analytics

Azer Bestavros

Computer Science Department

Hariri Institute for Computing

Boston University

BOSTON UNIVERSITY

Dataverse Privacy Workshop @ Harvard University

July 13, 2016

MPC in the land of social science with mayors, lawyers, CTOs, CIOs, administrators, politicians, journalists, and lawmakers…

A True Story by Azer Bestavros

BOSTON UNIVERSITY

July 31, 2014

Boston University Rafik B. Hariri Institute for Computing and Computational Science & Engineering

FOR IMMEDIATE RELEASE: September 23, 2014

CONTACT: Kira Jastive, 617-358-1240 or kjastive@bu.edu

(Boston) – Boston University's Rafik B. Hariri Institute for Computing and Computational Science & Engineering today announced it has received funding from the National Science Foundation (NSF) to develop a "smart-city" cloud platform designed to streamline and strengthen multiple municipal functions. Called *SCOPE: A Smart-city Cloud-based Open Platform & Eco-system*, the project is designed to improve transportation, energy, public safety, asset management, and social services in the City of Boston and across Massachusetts.

National Science Foundation
WHERE DISCOVERIES BEGIN

Press Release 14-089

Expanding the breadth and impact of cybersecurity and privacy research

NSF announces two Frontier-scale projects, part of a $74.5 million investment to support foundational cybersecurity research and education

July 31, 2014

Katharine Lusk

BU Initiative on Cities

INITIATIVE ON CITIES

The Initiative on Cities engages with urban leaders, academics, and policy makers from around the world to help plan for the development of essential services and sustainable infrastructure necessary for cities to flourish.

Meeting with Mayor Menino @ BU, July 31, 2014

April 9, 2013

WOMEN'S WORKFORCE COUNCIL

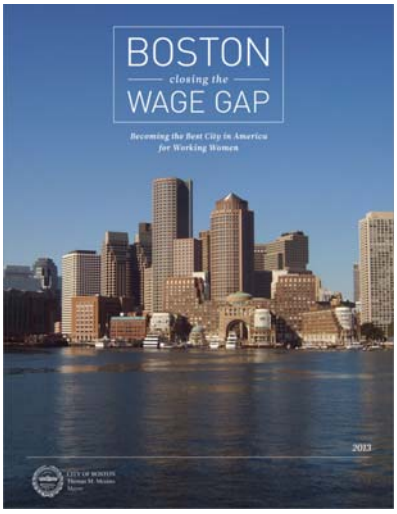
The Women's Workforce Council was established by Mayor Thomas M. Menino on April 9th, 2013— known nationwide as Equal Pay Day. The day marks how far into 2013 women need to work to earn what men earned in 2012. The first of its kind in the country, the Council's mission is to help transform Boston into the best city in the country for working women.

Members of the Council represent the financial, engineering, medical, law, technology and retail sectors, and include small business owners, entrepreneurs, senior executives, as well as academic, labor and nonprofit leaders.

The Council's first priority was to identify new and creative ways to help close the wage gap between working men and women, helping Boston become the first major city to achieve pay equity. This report outlines the Council's recommendations to employers throughout the city and across the region.

CATHY E. MINEHAN Dean of the School of Management, Simmons College [Chair]
TRICIA ADAMS Co-Owner, Marla's Obsessions
RUTH BRAMSON CEO, Girl Scouts of Eastern Massachusetts
VICTORIA A. BUDSON Executive Director, Women and Public Policy Program, Harvard Kennedy School
ELIZABETH HOENSCHEID CEO, Top it Off
DR. PAULA A. JOHNSON Chief, Division of Women's Health, Brigham & Women's Hospital; Executive Director, Connors Center for Women's Health and Gender Biology
TRISH KARTER CEO, LightEffect Farms
ZORICA PANTIC President, Wentworth Institute of Technology
KELLY PELLAGRINI Co-Founder, Charlestown Nursery School
ALISON A. QUIRK EVP, Chief of Human Resources and Corporate Citizenship, State Street
PRITI RAO Executive Director, Massachusetts Women's Political Caucus
MICHO SPRING President New England, Weber Shandwick
JENNIFER SPRINGER General Counsel, SEIU Local 888 and EVP-at-Large, Mass AFL-CIO
RAQUEL WEBSTER Senior Counsel, National Grid
BETH WILLIAMS CEO and President, Roxbury Technology Corp.
WENDY ZINN Executive Director, Huntington Avenue YMCA

October 31, 2013



CITY OF BOSTON · MASSACHUSETTS

OFFICE OF THE MAYOR
THOMAS M. MENINO

October 31, 2013

Dear Friends:

In 2013, I pledged to help close the wage gap between working men and women in Boston, as part of my efforts to make Boston the premier city for working women. This pledge is inspired by what we all know to be true: when Boston's women thrive, our city thrives – our employers are able to find the talent they need to excel, our many colleges and universities are dynamic and diverse, families are well cared for, and neighborhoods are active and communities are connected.

The persistent wage gap between working men and women presents an impediment to women's success, and thus of our great city. When women are undervalued and underpaid, it is harder for them to care for their families, pay off student loans and save for retirement. Women's choices and futures become limited, ultimately limiting the success and growth of our businesses and institutions.

I am proud of the tremendous advancements this city has made in my lifetime. Boston has broken down racial barriers and overcome the tragedy of segregation, and our state was the first in the nation to legalize gay marriage. Boston could now be the first major city to achieve pay equity. It will take employers working together, adopting proven interventions and inventing new ones.

I am grateful to the Women's Workforce Council for their leadership on pay equity. And I am excited about the recommendations outlined in this report and the opportunities Boston has to close the wage gap. Together, we've come so far. In 2013, it is time that we take this next great leap.

Sincerely,

Thomas M. Menino
Mayor of Boston

BOSTON CITY HALL • ONE CITY HALL PLAZA • BOSTON • MASSACHUSETTS 02201 • 617-635-4000

Source: http://www.cityofboston.gov/images_documents/Boston_Closing%20the%20Wage%20Gap_Interventions%20Report_tcm3-41353.pdf

December 11, 2013

100% TALENT

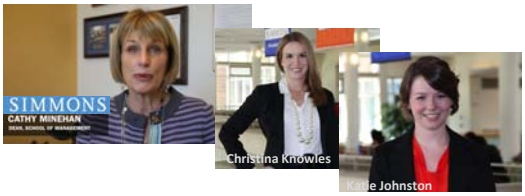
The Boston Women's Compact

To make Greater Boston the premier place for working women in America, by closing the wage gap and removing the visible and invisible barriers to women's advancement. By doing so, we will build a more equitable workforce where all talent is cultivated and valued.

GOAL 3
Evaluating Success
Employers agree to participate in a biennial review to discuss successes and challenges, as well as 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. The specific data to be reported will build on data already required by federal and state authorities and should not create an additional reporting burden.

GOAL 3
Evaluating Success
Employers agree to participate in a biennial review to discuss successes and challenges, as well as 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. The specific data to be reported will build on data already required by federal and state authorities and should not create an additional reporting burden.

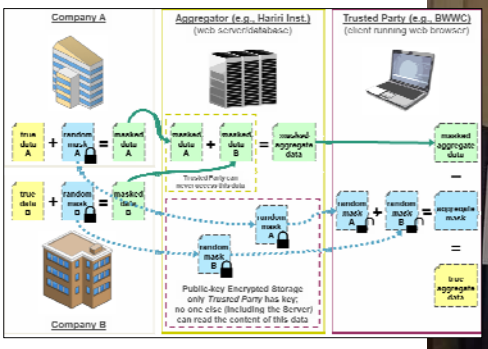
September 4, 2014

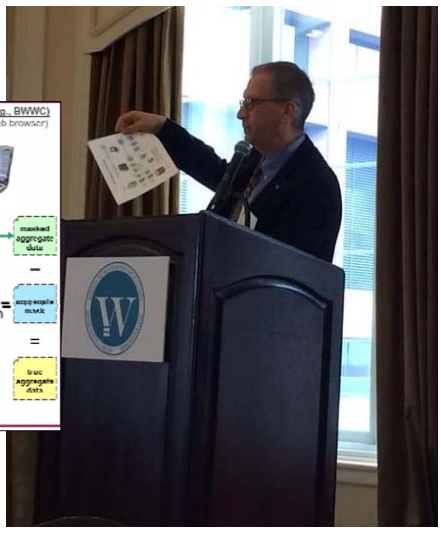


Snapshot of (a small subset of) BWWC meetings from Azer's Exchange Calendar

Subject	Start	Duration
Cathy Minehan	Fri 9/5/2014 10:30 AM	2 hours
Simmons College	Mon 10/27/2014 3:30 PM	1.5 hours
Data Collection for Pay Equity	Tue 12/2/2014 11:30 AM	30 minutes
Simmons College people	Fri 1/23/2015 1:00 PM	30 minutes
Invitation: 100% Talent Discussion with Data Partners @ Tue Mar 17, 2015 2pm - 3pm (johnstk3@s...	Tue 3/17/2015 2:00 PM	1 hour
Updated Invitation: MassMutual call with Hariri Institute re: Data Collection... @ Thu May 14, 2015 ...	Thu 5/14/2015 3:00 PM	1 hour
Invitation: Mock collection #1 @ Tue May 19, 2015 11am - 12pm (johnstk3@simmons.edu)	Tue 5/19/2015 11:00 AM	1 hour
Invitation: Mock Collection #2 @ Tue May 26, 2015 11am - 12pm (johnstk3@simmons.edu)	Tue 5/26/2015 11:00 AM	1 hour
Invitation: Mock Collection #3 @ Thu May 28, 2015 11am - 12pm (johnstk3@simmons.edu)	Thu 5/28/2015 11:00 AM	1 hour
Invitation: Call with BWWC @ Wed Jun 3, 2015 11:30am - 12pm (johnstk3@simmons.edu)	Wed 6/3/2015 11:30 AM	30 minutes
Updated Invitation: 100% Talent Data Collection: Hariri and Raytheon @ Fri Jun 5, 2015 9am - 10a...	Fri 6/5/2015 9:00 AM	1 hour
Invitation: 100% TALENT DATA COLLECTION @ Mon Jun 8, 2015 9am - 10:30am (johnstk3@simm...	Mon 6/8/2015 9:00 AM	1.5 hours
Invitation: Meeting with Boston Women's Workforce Council @ Tue Aug 11, 2015 10am - 11am (jo...	Tue 8/11/2015 10:00 AM	1 hour

April 14, 2015





April 14, 2015

The Boston Globe — Business

Mayor Walsh pushes to gather data on gender wage gap

Top 10 Trending Articles

After confidentiality concerns stalled Boston's gender pay initiative, computer scientist Azer Bestavros proposed an algorithm that solved the problem. Photo by Cydney Scott

BU Today — In the World

Computational Thinking Breaks a Logjam

Hariri Institute helps address Boston's male-female pay gap

Marty Walsh had a problem. Boston's mayor wanted to address pay disparities between men and women, publicizing, as a first step, the average gap in different Boston industries. Normally, calculating that gap would require taking the actual pay gap at each company in an industry, adding them up, and then dividing by the number of companies to reach an average. But companies' payrolls are proprietary, because their disclosure could be a boon to competitors, a black eye for the firms, and ammo for disgruntled employees who could sue over pay inequities.

Even if firms could trust a third party that swore secrecy to look at their numbers and calculate industry averages, hackers might breach that party's online security and steal these precious informational nuggets.

"So this project hit a hurdle," says Azer Bestavros, director of BU's Rafik B. Hariri Institute for Computing and Computational Science & Engineering. "It wasn't going to happen unless there was a way to do it, and there didn't seem to be a way."

June 6, 2015

BOSTON WOMEN'S WAGE COMPACT
DATA CONTRIBUTION AGREEMENT

This Data Contribution Agreement (the "**Agreement**"), effective as of June ___, 2015 (the "**Effective Date**"), is entered into by and among the Simmons College ("**Simmons**"), Boston University, through its Rafik B. Hariri Institute for Computing and Computational Science and Engineering ("**BU**") and State Street Bank and Trust Company ("**State Street**").

In consideration of the mutual covenants, terms and conditions set forth herein, and for other good and valuable consideration, the receipt and sufficiency of which are hereby acknowledged, the parties agree as follows:

1. Scope.

(a) The parties hereto wish to collaborate on a first-in-the-nation measurement that will capture the status of the gender wage gap within a set of companies. The parties desire to provide and collect data that will allow the wage gap to be measured in more precise ways. The results of the collaboration will be reflected in the resulting snapshot report ("**Report**") that will be completely anonymous with respect to the companies that provided data for the purposes thereof and will, in part, compare the status of the gender wage gap in the collaboration participants to that of all Boston employers, as written in the Boston Women's Workforce Council's 2013 Report, Boston Closing the Wage Gap.

(b) Each party undertakes to each other party to use reasonable endeavors to perform and fulfill, promptly and actively, all of its obligations under this Agreement. Each party will contribute to the efficient flow of information and access to relevant data to ensure the effectiveness and efficiency of this collaboration. Each party undertakes to use reasonable endeavors to (i) notify the other parties promptly of any significant delay in performance; and (ii) inform the other parties of relevant communications it receives from third parties in relation to this collaboration or this Agreement. Each party shall use reasonable endeavors to ensure the accuracy of any information or materials it supplies hereunder and promptly to correct any error therein of which it is notified. Each party shall be fully responsible for the supervision of its employees, agents and contractors and shall enter into appropriate arrangements for such purpose with its contractors. Each party will assign employees and/or other personnel of their respective organizations to carry out the work of the collaboration. Each employee and personnel assigned to work on the collaboration will continue to function in its role at the organization making the assignment. Each party will provide effective supervision for its employees and other personnel that they assign to collaborative activities and will retain responsibility and liability for the actions of such employees and other personnel. As among the parties to this Agreement, each party will be responsible for all costs and expenses incurred by such party in connection with this collaboration.

(c) The parties acknowledge and agree that the purpose and scope of this collaboration may be further refined and adjusted or changed throughout the Term (as defined below) by written agreement signed by each party. Any refinements, adjustments and changes shall be discussed in good faith amongst the parties and mutually agreed upon in writing prior to any party proceeding in a manner that reflects such refinements, adjustments or changes.

2. Data Contribution. State Street will deliver to Simmons and BU certain aggregate data, as agreed upon amongst the parties, for use in connection with this collaboration and the resulting Report (the "**Data**"). The Data shall be delivered in an agreed-upon format and using an agreed-upon method that provides security and anonymity with respect to the Data and the provider thereof. Each of Simmons and BU shall have established prior to receipt of any of the Data, and shall continue to maintain for so long as Data is in its possession or control, generally accepted industry "best practices" systems security measures designed to guard against the destruction, loss, or alteration, of the Data that are no less rigorous than those maintained by it for its own information. Simmons and BU shall each maintain adequate administrative, technological and procedural access controls and system security requirements and devices necessary to protect the Data from: (a) threats or hazards to the privacy, confidentiality or integrity of the Data; (b) unauthorized or unauthorized access to the Data; and (c) unlawful processing or accidental loss of, or destruction of or damage to, the Data.

3. Rights in the Data and Resultant Data.

(a) Simmons and BU each shall have the right to process and use the Data solely for purposes of the collaboration identified herein and in connection with the publication of the Report. Each of Simmons and BU hereby agree not to release specific information identifying State Street as a contributor of the Data or which identifies State Street as the source of the Data or any portion thereof. Simmons and BU will each bear the expense of incorporating the Data into the Report.

(b) The parties acknowledge and agree that State Street hold rights to, owns and/or controls the Data and any other data, information and/or materials that are or may be useful for purposes of the collaboration conducted herein. In addition, the parties acknowledge and agree that the Report shall not be published or otherwise disclosed prior to State Street's approval of the final version of the Report.

(c) Simmons and BU each have, reserve and retain all right, title and interest in and to all data, information, materials and other content of any type and in any format, medium or form that is processed by, for or on behalf of it by or through any device, system or network, including, but not limited to, any and all works, inventions, data, analyses and other information and materials resulting from the activities contemplated by this Agreement and all output, copies, reproductions, improvements, modifications, adaptations, translations and other derivative works thereof, based thereon or derived therefrom, other than the Data contributed hereunder (collectively, the "**Resultant Data**").

(d) Nothing contained in this Agreement will be construed as granting, by implication, waiver, estoppel or otherwise to Simmons and/or BU any right, title or interest in or to the Data, except for the limited rights expressly granted to each Simmons and BU pursuant to this Agreement.

4. Confidentiality.

(a) "**Confidential Information**" means information that the Disclosing Party (as defined below) treats as confidential or proprietary, including, but not limited to, trade secrets, technology, information pertaining to business operations and strategies, and information pertaining to customers, pricing and that confidential treatment will be afforded the Confidential Information.

5. Warranties.

(a) Each party represents and warrants to each other party that: (i) it has the full right, power and authority to enter into this Agreement and to perform its obligations hereunder; (ii) when executed and delivered by the party, this Agreement shall constitute the legal, valid and binding obligation of that party, enforceable against that party in accordance with its terms; and (iii) it is under no obligation to any third party that would interfere with its obligations under this Agreement.

(b) State Street has the unconditional and irrevocable right, power and authority to grant the rights hereunder to the Data pursuant to the terms of this Agreement; and

(c) EXCEPT AS EXPRESSLY SET FORTH ABOVE, TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, EACH PARTY HEREBY DISCLAIMS ALL WARRANTIES, WHETHER EXPRESS, IMPLIED, STATUTORY OR OTHERWISE, WITH RESPECT TO THIS AGREEMENT OR ANY SUBJECT MATTER HEREOF, INCLUDING, WITHOUT LIMITATION, ANY WARRANTY OF NON-INFRINGEMENT.

6. Limitations of Liability. TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, IN NO EVENT WILL ANY PARTY BE LIABLE FOR ANY LOSS OF, DAMAGE TO, OR CORRUPTION OF DATA, LOST PROFITS, BUSINESS, CONTRACTS, REVENUE, PRODUCTION, GOODWILL, OR ANTICIPATED SAVINGS, OR BUSINESS INTERRUPTION, OR OTHER COMMERCIAL, ECONOMIC OR OTHER DAMAGES, ARISING ON INJURY OF ANY KIND, INCLUDING, BUT NOT LIMITED TO, ANY INDIRECT, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF OR IN CONNECTION WITH THIS AGREEMENT OR ANY SUBJECT MATTER HEREOF, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH LOSSES, DAMAGES OR INJURIES AND REGARDLESS OF WHETHER ANY REMEDY SET FORTH IN THIS AGREEMENT FAILS OF ITS ESSENTIAL PURPOSE. The limitations of damages set forth herein does not apply to a party's obligations under Sections 3 or 4 or in the event of a party's gross negligence, willful misconduct or fraud.

7. Term and Termination.

(a) This Agreement commences as of the Effective Date and will continue in effect until terminated as provided herein (the "**Term**").

(b) Any party may terminate this Agreement:

(i) at any time, without cause, and without incurring any obligation, liability or penalty by reason of such termination, upon at least thirty (30) days' prior written notice to the other parties; or

(ii) upon written notice to the other parties in the event that another party hereto has committed a material breach of the terms of this Agreement and such party has not cured such breach within thirty (30) days after receiving written notice of such breach from a non-breaching party.

(c) upon the expiration of the Term or the termination of this Agreement in accordance with this Section 7, each party shall (i) immediately discontinue all use of Confidential Information of any other party obtained hereunder; and (ii) promptly return or cause to be returned to such other party or destroy or cause to be destroyed all copies obtained, made or authorized to be made hereunder of documents and tangible materials containing, reflecting, incorporating or based on any Confidential Information of such other party, and certify in writing to such other party that it

Any purported assignment, delegation or transfer in violation of this Section is void. This Agreement is binding upon and inures to the benefit of the parties hereto and their respective permitted successors and assigns.

(c) Amendment; Waiver. This Agreement may only be amended, modified or supplemented by an agreement in writing signed by each party hereto. No waiver by any party of any of the provisions hereof shall be effective unless explicitly set forth in writing and signed by the party so waiving.

(f) Severability. If any term or provision of this Agreement is invalid, illegal or unenforceable in any jurisdiction, such invalidity, illegality or unenforceability shall not affect any other term or provision of this Agreement.

(g) Governing Law; Jurisdiction. This Agreement shall be governed by and construed in accordance with the internal laws of the Commonwealth of Massachusetts, without giving effect to any choice or conflict of law provision or rule. Neither the United Nations Convention on the International Sale of Goods nor the Uniform Computer Information Transactions Act shall have any application to this Agreement. Any legal suit, action or proceeding arising out of or related to this Agreement shall be instituted exclusively in the federal courts of the United States or the courts of the Commonwealth of Massachusetts in each case located in the city of Boston, and each party irrevocably submits to the exclusive jurisdiction of such courts in any such suit, action or proceeding.

(h) Equitable Remedies. Each party to this Agreement acknowledges and agrees that (i) a breach or threatened breach by such party of any of its obligations under this Agreement may give rise to irreparable harm to the other party for which monetary damages would not be an adequate remedy, and (ii) in the event of a breach or a threatened breach by such party of any such obligations, the other party shall, in addition to any and all other rights and remedies that may be available to such party at law, at equity or otherwise in respect of such breach, be entitled to seek equitable relief, without any requirement to post a bond or other security or to prove actual damages or that monetary damages will not afford an adequate remedy.

(i) Export Regulations. Simmons and BU each acknowledge and agree that it shall not export, or re-export directly or indirectly, the Data, to any country or person in violation of the laws and regulations of any applicable jurisdiction, which restriction expressly includes, but is not limited to, the export regulations of the United States of America.

Agreement effective as of the date first above written.

Boston University, through its Rafik B. Hariri Institute for Computing and Computational Science and Engineering

By: _____

Name: _____

Title: _____

Boston University, through its Rafik B. Hariri Institute for Computing and Computational Science and Engineering

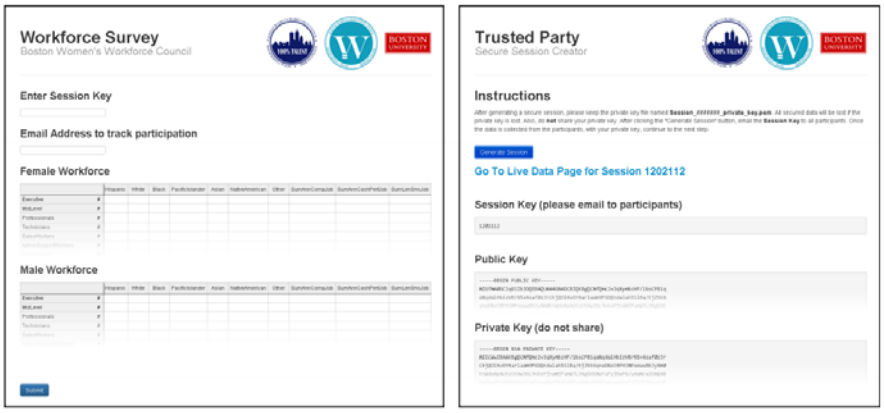
By: _____

Name: Thane M. Kreiner

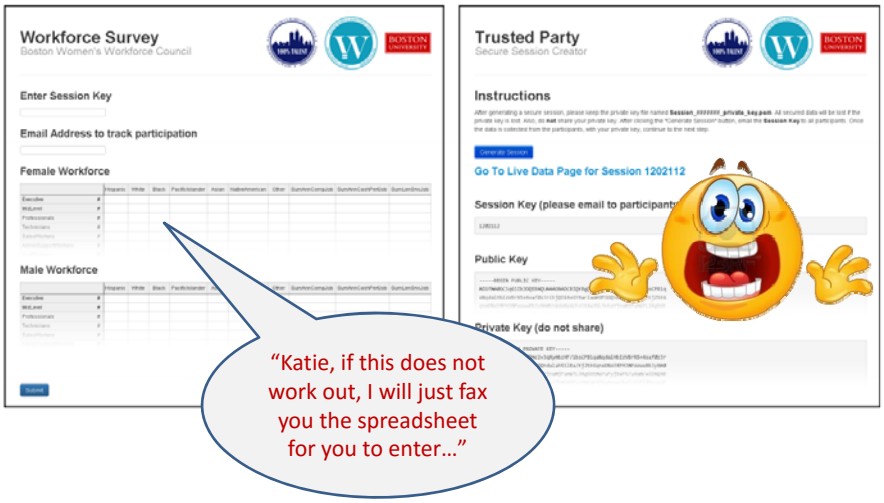
Title: Assistant Vice President, Sponsored Programs

6/17/15

June 8, 2015
D-day



June 8, 2015
D-day



September 29, 2015

Tweets Tweets & replies

Azer Bestavros @Bestavros · Sep 29

Grateful to @RepKClark for her advocacy of @NSF funding and its broader impacts and thanks @BUFederal for hosting me

BU Federal Relations @BUFederal

Loved meeting w/ @RepKClark & @BU_Computing head Azer Bestavros re: #smartcities #NSF #equalpay

2

Azer Bestavros

Yesterday at 6:26pm

In DC, with Massachusetts 5th District (my district) Representative Congresswoman Katherine Clark -- a true advocate for NSF funding and for gender pay equity. I was there to tell her how these two got connected through an Institute project!

October 20, 2015

'You have to respect the fact that policy makers . . . don't talk your lingo.'

ALAN ALDA, *actor and founder of center for communicating science*

Making discoveries, then making them clear

Theater exercises help BU scientists reach vital audiences

By Tracy Jan

GLOBE STAFF

The men and women stared intently into their partner's eyes, slowly stretching their arms and bending to the side, in a silent and mysterious dance. They struggled to stifle giggles as they mirrored each other's awkward movements.

The improvisational theater game was designed to train them to pay

Scientists learn to reach audiences

▶SCIENTISTS

Continued from Page A1

Dartmouth College, University of Vermont, and University of Maine, along with a growing number of other universities.

These days, scientists' groundbreaking discoveries are no longer enough. More than ever, in a new era of federal austerity, scientists must be able to succinctly communicate how their work can change lives. They must learn to speak eloquently and passionately before congressional committees, government officials, and private philanthropists about the societal benefits of investing in research.

"We are in fiscally restrained

DREW ANGERER FOR THE BOSTON GLOBE

Computer science professor Azer Bestavros explained his work to Representative Katherine Clark in Washington.

On a recent morning, Bestavros and a Washington lobbyist for BU sat in the Capitol Hill office of Representative Katherine Clark, a Massachusetts Democrat on the House committee that oversees funding for the National Science Foundation.

Bestavros wanted to thank her for pushing for recent funding, impress upon her the importance of continued support, and arm Clark with ammunition for future budget and policy fights.

"I don't want to bore you with the details of what we do," he said, before launching into a story of how he uses cloud com-

The Boston Globe

The congresswoman, who had signed onto a bill addressing income disparity between men and women, was impressed by the relevance he outlined. *"It's linking it back for the members of Congress,"* Clark said. *"Nobody would think, oh, the Paycheck Fairness Act, how is that tied into NSF funding?"*

The meeting was slated for 15 minutes. It lasted 25.

April 28, 2016

GOAL 3

Evaluating Success

Employers agree to participate in a biennial review to discuss successes and challenges, as well as 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. The specific data to be reported will build on data already required by federal and state authorities and should not create an additional reporting burden.

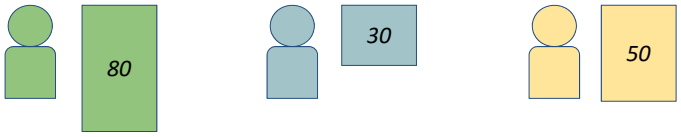
The Sequel

- Compact doubled in size
- More elaborate analytics
- Hardened user interface
- Provide local sanity checks
- Provide comparative metrics

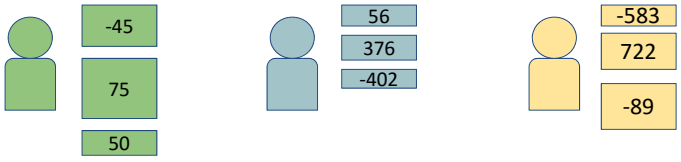
Multi-Party Computation (MPC)

- What is it?
  - Given multiple parties p_1, p_2, …, p_n each with private data x_1, x_2, …, x_n
  - Engage parties in a protocol to compute a function $f(x_1, x_2, …, x_n)$ without revealing more than the outputs of f
- State of the Art
  - Theory known for many decades, starting with Shamir's "How to share a secret" in 1979
  - Frameworks and libraries increasingly available over the last few years, e.g., VIFF, Sharemind, Oblivm, …
  - Experience with use cases involving real applications is limited and deployments are not easily portable

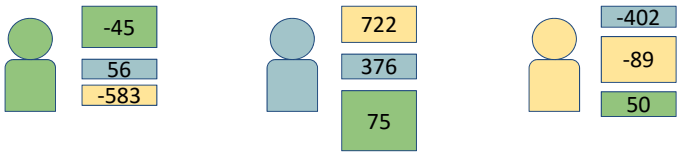
Example: Sum of Secret Records



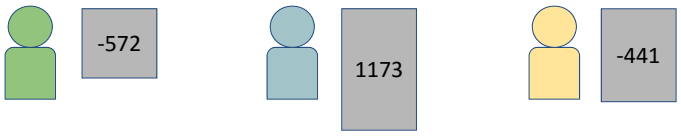
Players split secrets into “shares”



All players exchange shares



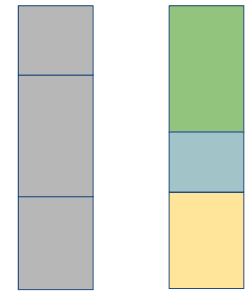
Each player the sum to obtain a share of the sum of secrets!



Exchange/combine to get result

Sum = 160

Lo and behold



Sum = 160 Sum = 160

The Parties in our MPC Setting

Contributors

- Have private data needed for computing the analytic
- Number of contributors is unknown in advance

Analyzers

- Ultimate recipient of the output of the analytic
- May also help in computing the analytic

Service Provider

- Connects/coordinate largely decoupled parties
- Has capacity to (partially) compute the analytic

Trust Assumptions

Contributors & analyzers place some trust in each other

- Analyzers trust that contributors will submit valid data
- Contributors trust that analyzers will protect aggregate output
- Contributors trust that analyzers will not collude with others

No trust in service provider

- Service provider cannot be entrusted with data or with the results of the computation
- Assume that service provider is incentivized to perform the computation on behalf of the contributors and analyzers

Operational Constraints

Comprehensibility of the Protocol
- MPC protocol must be simple for users (and lawyers/executives) to understand (and approve)

Auditability of the Service
- All software and processes must be transparent, with open-source code for outside auditing

Capability of Contributor/Analyzers Infrastructures
- Software clients must require no setup, no specialized software/hardware, or even public IP

Simplicity of Client Interfaces
- Usable by employees only familiar with spreadsheet application and web browsers

Asynchronicity
- Contributors need to be online while entering their data; analyzers to start/finish process

Idempotence
- Contributors must be able to resubmit/update their data to recover from errors, crashes, etc.

Feedback
- Interface for contributors must provide means to alert human users about spurious data

Putting it Together: Our Protocol

Let G be an appropriate additive group such as $\mathbb{Z}/2^{64}\mathbb{Z}$ and distinguish each contributor using an index $i \in \{1, ..., n\}$. We call a single execution of the protocol a *session* and it proceeds in the following way:

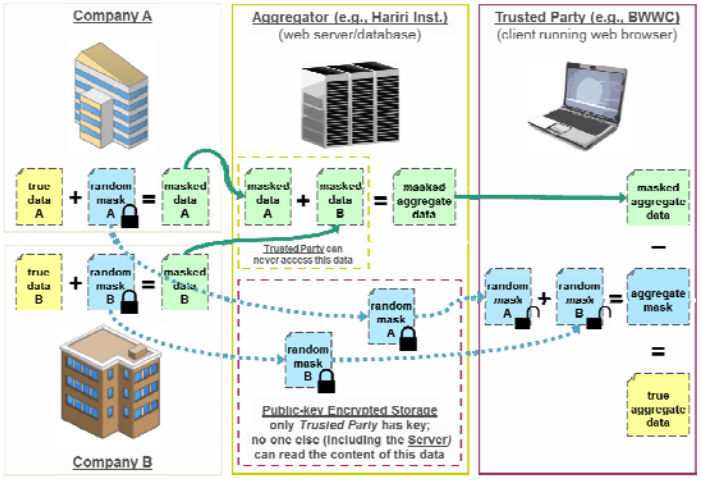
(1) the analyzer initiates the process by generating a secret and public RSA key pair (s, p) and a unique session identifier $j \in \mathbb{N}$, submitting p to the service provider, and sending j to all the contributors;[3]

(2) each of the n contributors possesses a secret *data* value $d_i \in G$ and does the following at least once[4]:
   (a) generate a secret *random mask* $m_i \in G$ and calculate the *masked data* $r_i = d_i + m_i$,
   (b) send r_i to the service provider and retrieve p from the service provider to send back $c_i = \mathrm{Enc}_p(m_i)$;

(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 analyzer 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 $R - M = \sum_{i=1}^{n} d_i$.

Web-Based MPC Platform

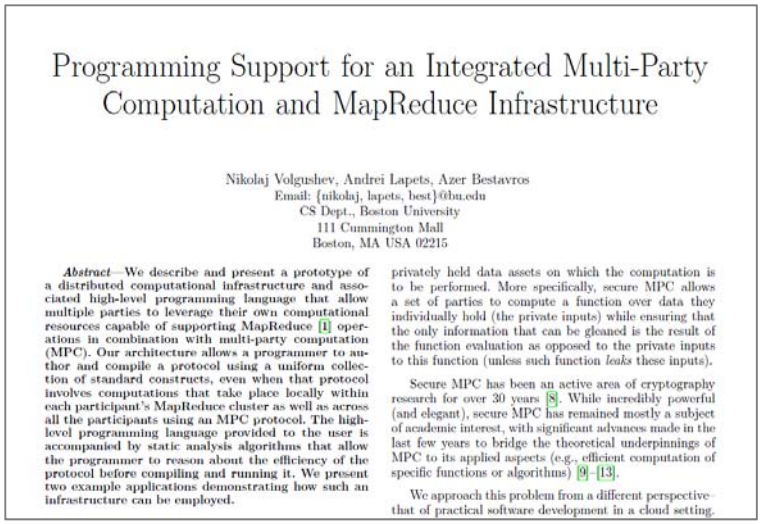


Open Source Software available at https://github.com/Boston-Women-Work

Bigger Picture: MPC as a Service

- Observations:
  - Data analysts should not be expected to worry about privacy or performance tradeoffs
  - Unrealistic to expect cryptographers to rewrite the huge existing corpus of privacy-agnostic analytics
  - Need to provide separate levers to manage privacy, utility, and performance tradeoffs
- Our Hypothesis (and research agenda):
  - MPC must be integrated seamlessly into popular, scalable data analytics platforms, e.g., MapReduce and Musketeer

MPC as a (cloud) Service



Programming Support for an Integrated Multi-Party Computation and MapReduce Infrastructure

Nikolaj Volgushev, Andrei Lapets, Azer Bestavros
Email: {nikolaj, lapets, best}@bu.edu
CS Dept., Boston University
111 Cummington Mall
Boston, MA USA 02215

***Abstract*—We describe and present a prototype of a distributed computational infrastructure and associated high-level programming language that allow multiple parties to leverage their own computational resources capable of supporting MapReduce [1] operations in combination with multi-party computation (MPC). Our architecture allows a programmer to author and compile a protocol using a uniform collection of standard constructs, even when that protocol involves computations that take place locally within each participant's MapReduce cluster as well as across all the participants using an MPC protocol. The high-level programming language provided to the user is accompanied by static analysis algorithms that allow the programmer to reason about the efficiency of the protocol before compiling and running it. We present two example applications demonstrating how such an infrastructure can be employed.**

privately held data assets on which the computation is to be performed. More specifically, secure MPC allows a set of parties to compute a function over data they individually hold (the private inputs) while ensuring that the only information that can be gleaned is the result of the function evaluation as opposed to the private inputs to this function (unless such function *leaks* these inputs).

Secure MPC has been an active area of cryptography research for over 30 years [8]. While incredibly powerful (and elegant), secure MPC has remained mostly a subject of academic interest, with significant advances made in the last few years to bridge the theoretical underpinnings of MPC to its applied aspects (e.g., efficient computation of specific functions or algorithms) [9]–[13].

We approach this problem from a different perspective– that of practical software development in a cloud setting.

MPC is great! But…

- MPC = math turtle shell for confidential data!
- Practical MPC frameworks exist, but
  - They are slow (not unlike turtles)
  - Learning curve is steep (trust me!)
- Lots of special-purpose gadgetery (circuits)
  - Apply to very narrow functions
  - Not for human consumption

MapReduce (MR): fast, like a hare!

- A programming paradigm for data analytics
  - Very easy to us (I teach it one lecture)
- Supported by distributed & elastic backend
  - Very easy to deploy (thanks to the cloud)
- Performance is ridiculously fast
  - 200 node cluster sorted 100TB of data in 23 minutes; think what 8,000 nodes can do!

Our Research

Separation of concerns
- Domain experts specify analytics as MR code
- Lawyers specify confidentiality constraints on data

Automate the interaction
- Compile the MR code subject to constraints
- Expose cost-privacy tradeoffs to resolve tussle

Build an execution platform
- Extend MR backend (SPARC) to support MPC
- Act as a platform to plug in special MPC gadgetry

The Scather Platform

A Programming Language

- To specify MR and MPC operations
- Not meant for consumption by non-experts

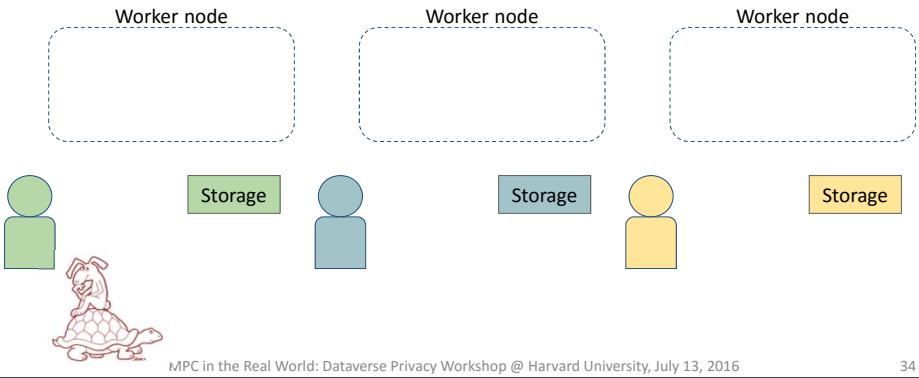
A Compiler

- To convert MR programs into Scather programs
- To expose tradeoffs

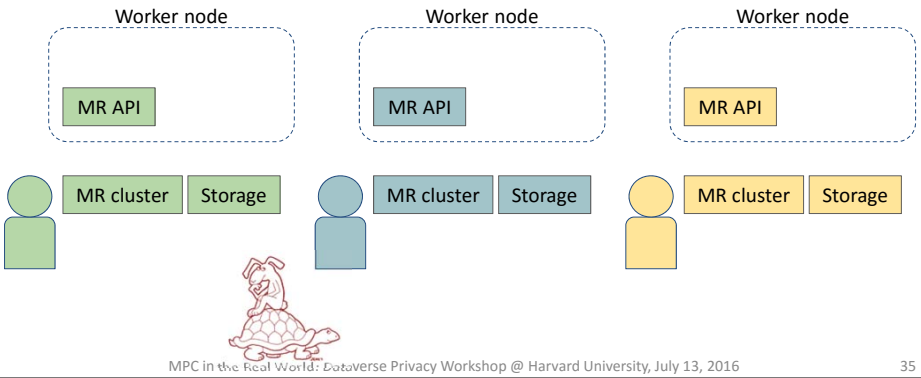
Backend Platform

- To run the show

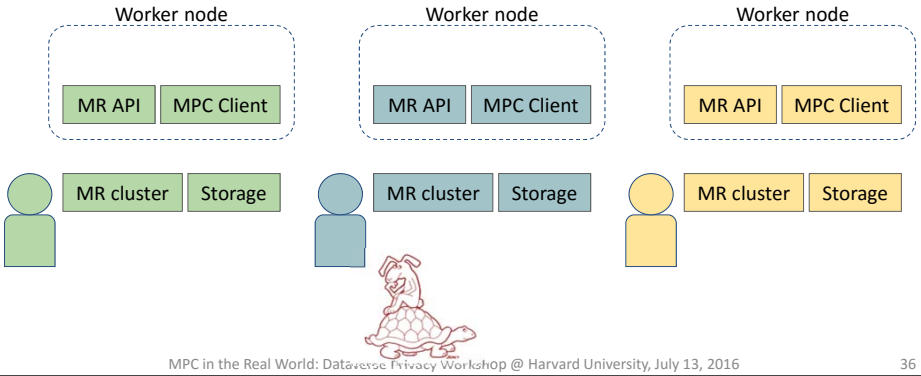
Data Secured in Local Safes



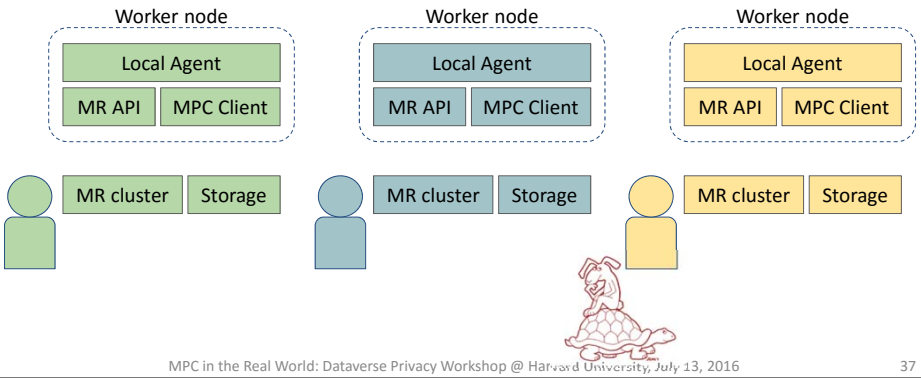
+ MapReduce Local Infrastructure



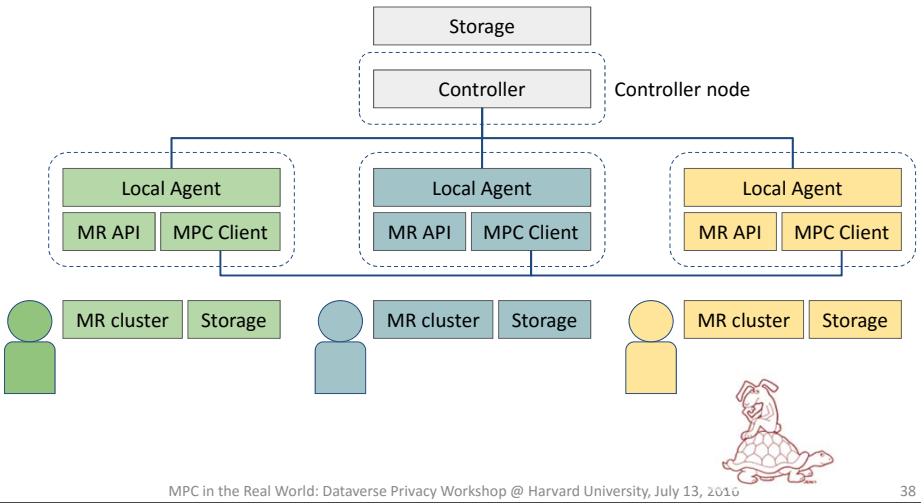
+ Local MPC Client



+ Local Agent to Manage MR-MPC

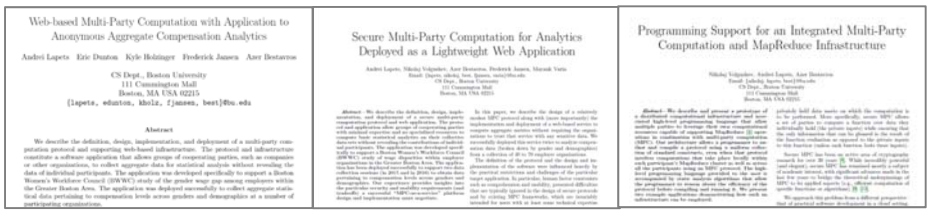


+ Controller for MP Coordination



MPC as a Service

Azer Bestavros Andrei Lapets Kyle Holzinger Eric Dunton Frederick Jansen Nikolaj Volgushev Mayank Varia



Web-based Multi-Party Computation with Application to Anonymous Aggregate Compensation Analytics

Andrei Lapets Eric Dunton Kyle Holzinger Frederick Jansen Azer Bestavros

CS Dept., Boston University
111 Cummington Mall
Boston, MA USA 02215
{lapets, edunton, kholz, fjansen, best}@bu.edu

Abstract

We describe the definition, design, implementation, and deployment of a multi-party computation protocol and supporting web-based infrastructure. The protocol and infrastructure constitute a software application that allows groups of cooperating parties, such as companies or other organizations, to collect aggregate data for statistical analysis without revealing the data of individual participants. The application was developed specifically to support a Boston Women's Workforce Council (BWWC) study of the gender wage gap among employers within the Greater Boston Area. The application was deployed successfully to collect aggregate statistical data pertaining to compensation levels across genders and demographics at a number of participating organizations.

Secure Multi-Party Computation for Analytics Deployed as a Lightweight Web Application

Programming Support for an Integrated Multi-Party Computation and MapReduce Infrastructure

MPC in the Real World

- Boston Globe: *Mayor Walsh pushes to gather data on wage gap* https://goo.gl/B7Kj79
- BU Today: *Computational Thinking Breaks a Logjam* http://goo.gl/dnsqbo
- BU Research Magazine: *Calculating Gender Pay Equity* http://goo.gl/y6hIWH
- NPR OnPoint: *Will Data Help Close The Gender Pay Gap?* http://goo.gl/2JIthb
- Boston Globe: More Boston businesses join drive to end gender wage gap https://goo.gl/xbEKuX