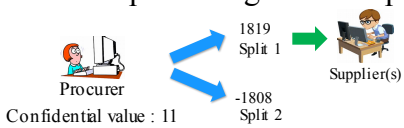
Computing without Revealing: A Cryptographic Approach to eProcurement

Siva C Chaduvula, PhD Student, Purdue University

Abstract

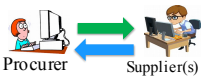
- Current eProcurement processes offer security against external attacks
- Information leak through procurement partners has increased over the recent years
- How can procurers and suppliers securely conduct their business transactions without revealing their confidential information?
- Our approach: Perform computations involved in procurement using lightweight secure multi-party computation (LSMC) techniques.

1. Hide inputs using additive splits



2. Compute over additive splits

3. Share additive splits of outputs



Our framework

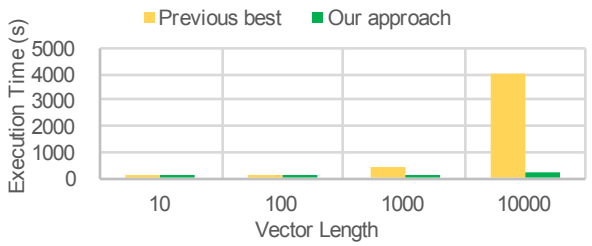
Methods

- Design Goals for procuring commodity-type products
  - Procurer need not reveal requirements to anyone
  - Suppliers need not reveal item prices to anyone
  - Procurer is able to "cherry pick" Suppliers with best prices for each individual requirement
  - Payments are made through Payment Center (a trusted third party) who learns only payment info
  - Payment Center does not learn about the context
  - Supplier(s) cannot be able to determine Procurer's requirements from payments
- Design Goals for specialized or custom products
  - Process enables Procurer to assess Supplier's capabilities
  - Process enables Procurer and Supplier(s) to negotiate a price with minimal disclosure of info

Results

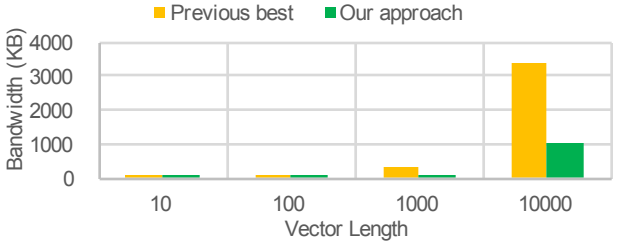
Execution Time (s) by Procurer

Vector length	0-server (PHE)	3-servers (Previous best)	1-server (Our approach)
10	14.6	4.1	0.35
100	135.5	37.4	2.88
1000	1738.4	378	27.5
10000	>3600	4031	264.7



Bandwidth Usage (KB) by Procurer

Vector length	0-server (PHE)	3-servers (Previous best)	1-server (Our approach)
10	6.5	3.4	1.18
100	61.8	33.8	10.6
1000	614.2	342.7	105.9
10000	>5000	3425.3	1053.7



PHE stands for Partial Homomorphic Encryption (Key length: 512 bits)

Note: Experiments are conducted using a 10Mbps LAN

Acquisition Research Program
Graduate School of Business & Public Policy
www.acquisitionresearch.net

Advisors: Dr. Jitesh H. Panchal, Purdue University
Dr. Mikhail J. Atallah, Purdue University
Acknowledgments: N00244-17-1-0009, NSF CPS 1329979