Computing without Revealing: A Cryptographic Approach to eProcurement

Siva C. Chaduvula

(Presented by Adam Dachowicz)

Jitesh H. Panchal

Associate Professor

Mikhail J. Atallah

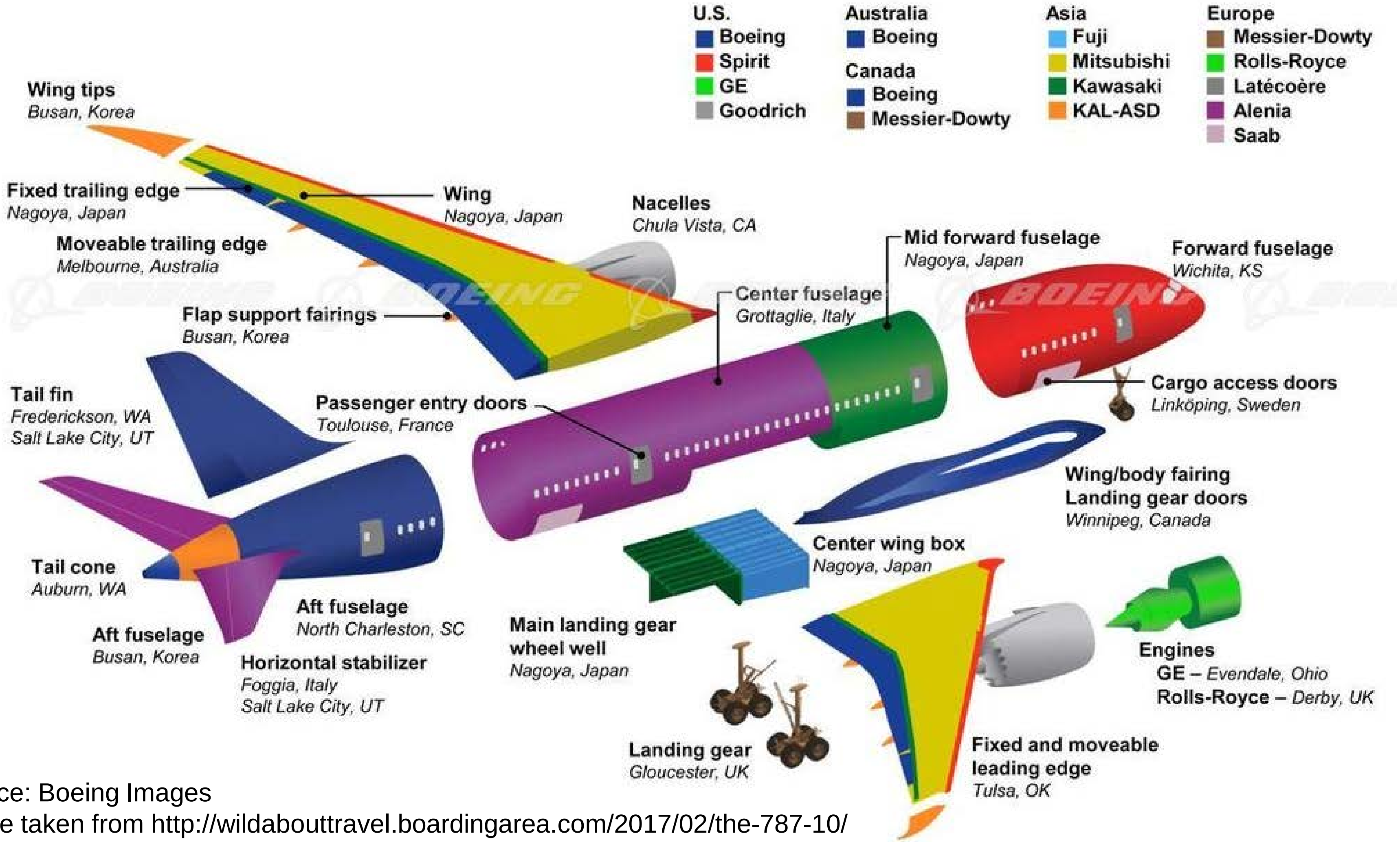
Distinguished Professor

May 8, 2019

16th Annual Acquisition Research Symposium
Panel No: 7
NPS Grant: N00244-17-1-0009

Design Engineering Laboratory @ Purdue
http://engineering.purdue.edu/DELP

Paradigm of engineering collaborations



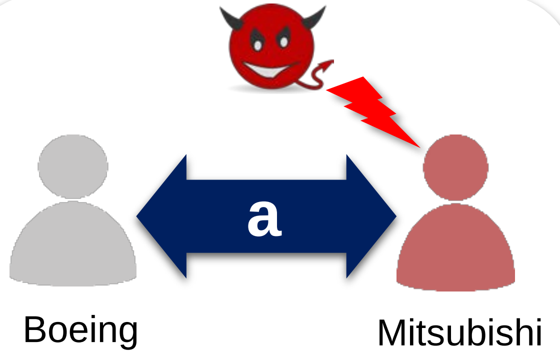
Source: Boeing Images
Image taken from http://wildabouttravel.boardingarea.com/2017/02/the-787-10/

Multiple suppliers contribute to the design & making of complex products

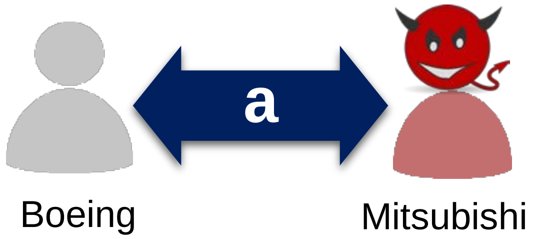
Need for security

Internal Attacks

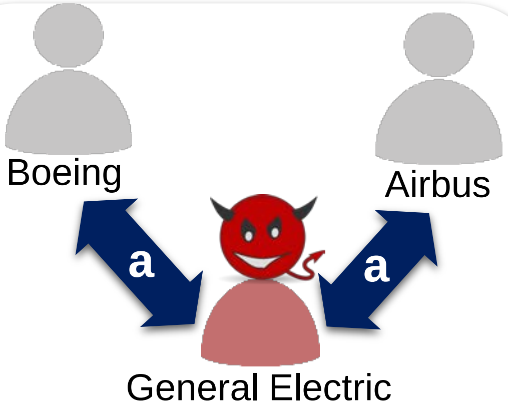
External Attacks



1. Vulnerable collaborator



2. Future competitor

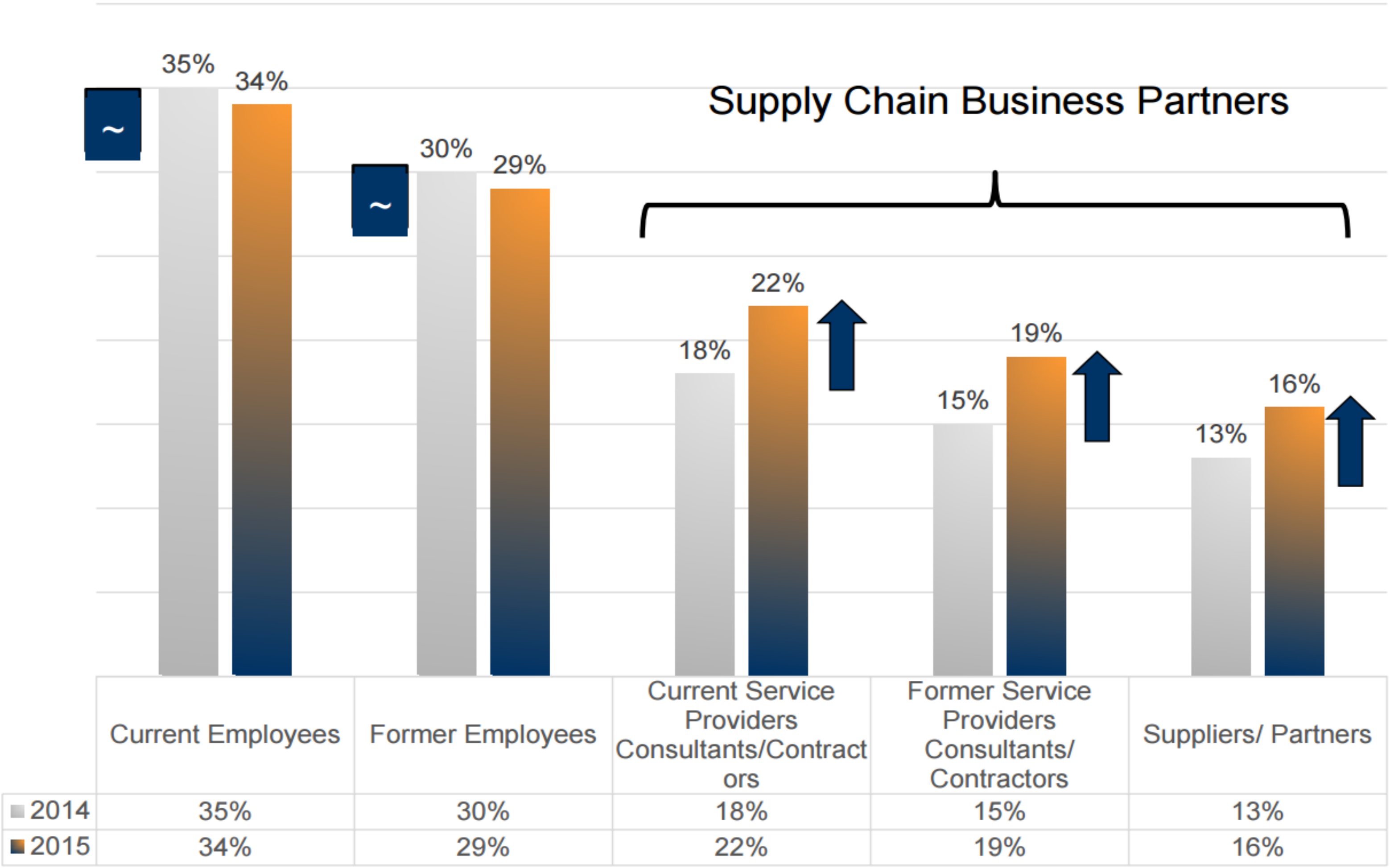


3. Common collaborator

Note: Enterprises mentioned in this slide are purely for illustrative purposes

Revealing sensitive data to collaborating designers amplifies risk of leakage and leads to unintended consequences

Increasing risk with business partners



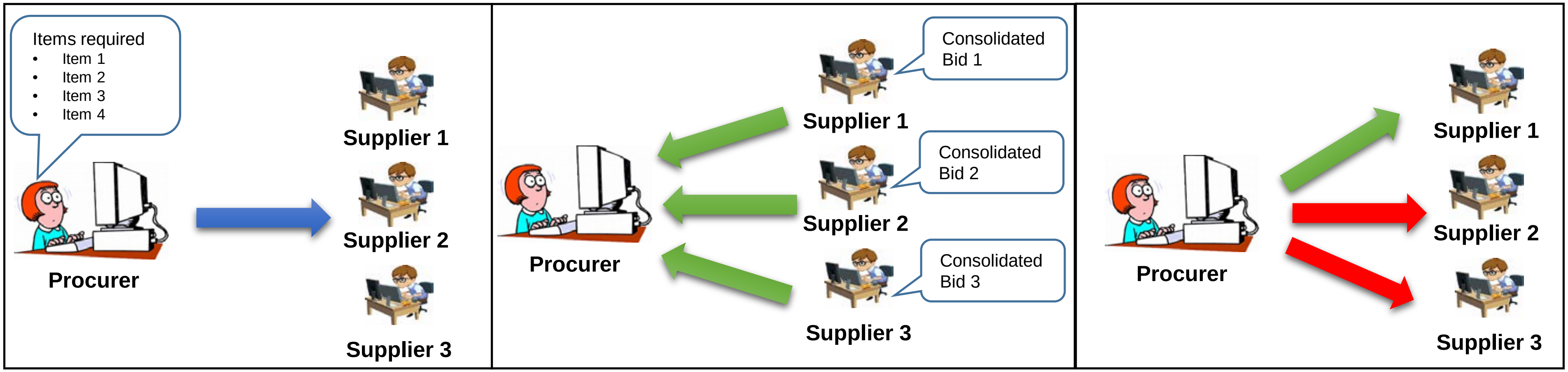
	Current Employees	Former Employees	Current Service Providers Consultants/Contractors	Former Service Providers Consultants/ Contractors	Suppliers/ Partners
▨ 2014	35%	30%	18%	15%	13%
▨ 2015	34%	29%	22%	19%	16%

* Adapted from the PwC *The Global State of Information Security® Survey 2016,*

Preserving data confidentiality is important while working with prospective, current, and past partners

Challenges with eProcurement of Standard Products

Example: Sealed Bid Auction



Items required
- Item 1
- Item 2
- Item 3
- Item 4

Procurer

Supplier 1

Supplier 2

Supplier 3

Procurer

Supplier 1

Consolidated Bid 1

Supplier 2

Consolidated Bid 2

Supplier 3

Consolidated Bid 3

Procurer

Supplier 1

Supplier 2

Supplier 3

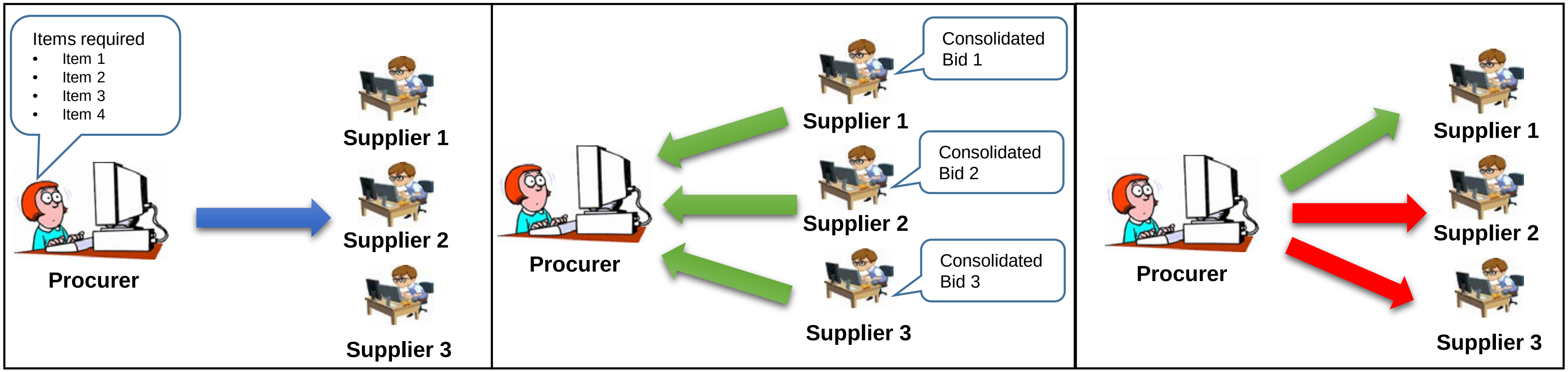
1. Broadcast the desired items

2. Interested suppliers submit consolidated bids

3. Procurer selects the supplier

Challenges with eProcurement of Standard Products

Example: Sealed Bid Auction



Items required
- Item 1
- Item 2
- Item 3
- Item 4

Procurer

Supplier 1

Supplier 2

Supplier 3

Procurer

Supplier 1

Consolidated Bid 1

Supplier 2

Consolidated Bid 2

Supplier 3

Consolidated Bid 3

Procurer

Supplier 1

Supplier 2

Supplier 3

Procurer Needs:

A

B

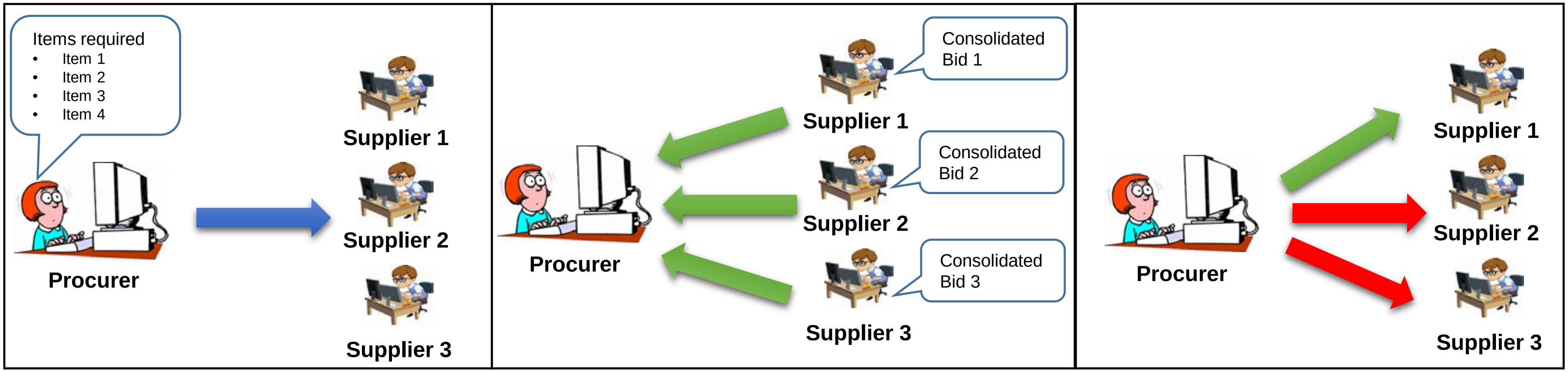
C

	Supplier 1	**Supplier 2**	**Supplier 3**
A	$ 10,000	$ 15,000	$ 11,000
B	$ 7,000	$ 4,000	$ 4,500
C	$ 20,000	$ 23,000	$ 30,000

Revealing price points for individual items hurts suppliers in the long term

Challenges with eProcurement of Standard Products

Example: Sealed Bid Auction



1. Broadcast the desired items

2. Interested suppliers submit consolidated bids

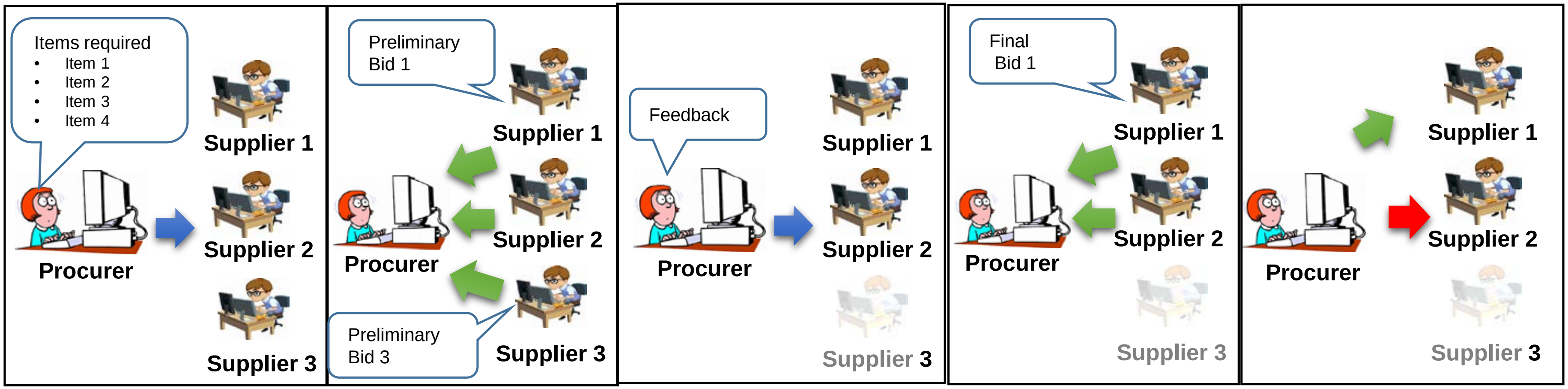
3. Procurer selects the supplier

Challenges:

1. Procurer needs to reveal their desired items and quantities to the prospective suppliers
2. Suppliers need to reveal their bids to the procurer or a trusted third party (TTP)
3. Procurer cannot choose best price for each individual item

Challenges with eProcurement of Innovative Technology

Example: Two-Stage Auction (Iterated Information Aggregation Auction[1])



Items required
- Item 1
- Item 2
- Item 3
- Item 4

Procurer

Supplier 1

Supplier 2

Supplier 3

Preliminary Bid 1

Procurer

Supplier 1

Supplier 2

Supplier 3

Preliminary Bid 3

Feedback

Procurer

Supplier 1

Supplier 2

Supplier 3

Final Bid 1

Procurer

Supplier 1

Supplier 2

Supplier 3

Procurer

Supplier 1

Supplier 2

Supplier 3

1. Broadcast the cost parameters

2. Submission of Cost/Quality Bids

3. Eliminate low value bidders

4. Update Cost/ Quality Bids

5. Select the highest value bidder

Challenge: Suppliers need to disclose their confidential information to the procurer without any guarantee of a contract

Research Question: **How can procurers and suppliers securely conduct business transactions without revealing their confidential data?**

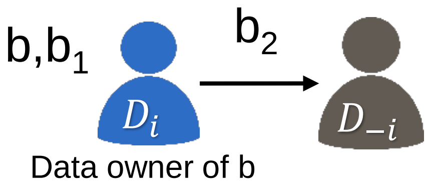
[1] Coughlan, Peter, William Gates, and Jennifer Lamping. Innovations in defense acquisition auctions: Lessons learned and alternative mechanism designs. No. NPS-AM-08-013. Naval Postgraduate School Monterey CA Graduate School of Business and Public, 2008.

Approach: Computing without Revealing (CWR)

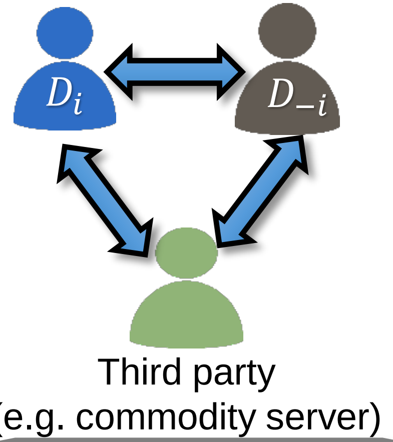
1. Split the input & send the input share

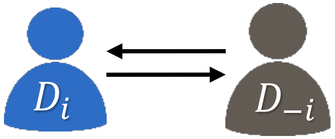
2. Perform computations with the help of a third party on the input shares

3. Reveal output shares as appropriate



$$b_1 = b - r \ (|r| \gg b)$$
$$b_2 = r$$
$$b = b_1 + b_2$$





Foundational CWR Protocols[1]

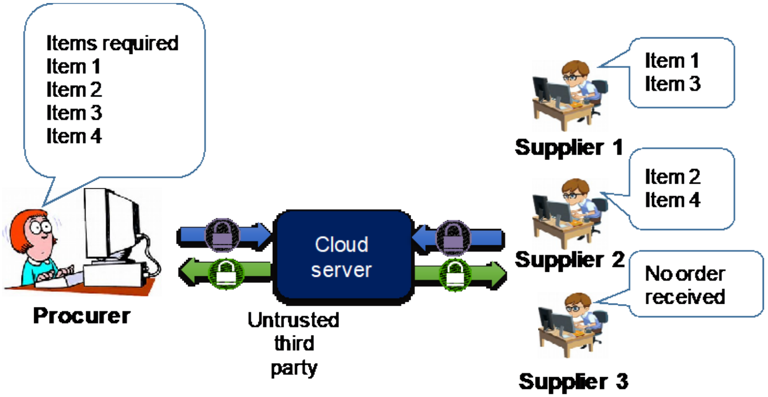
Arithmetic Operations
- **Addition**
- **Multiplication**

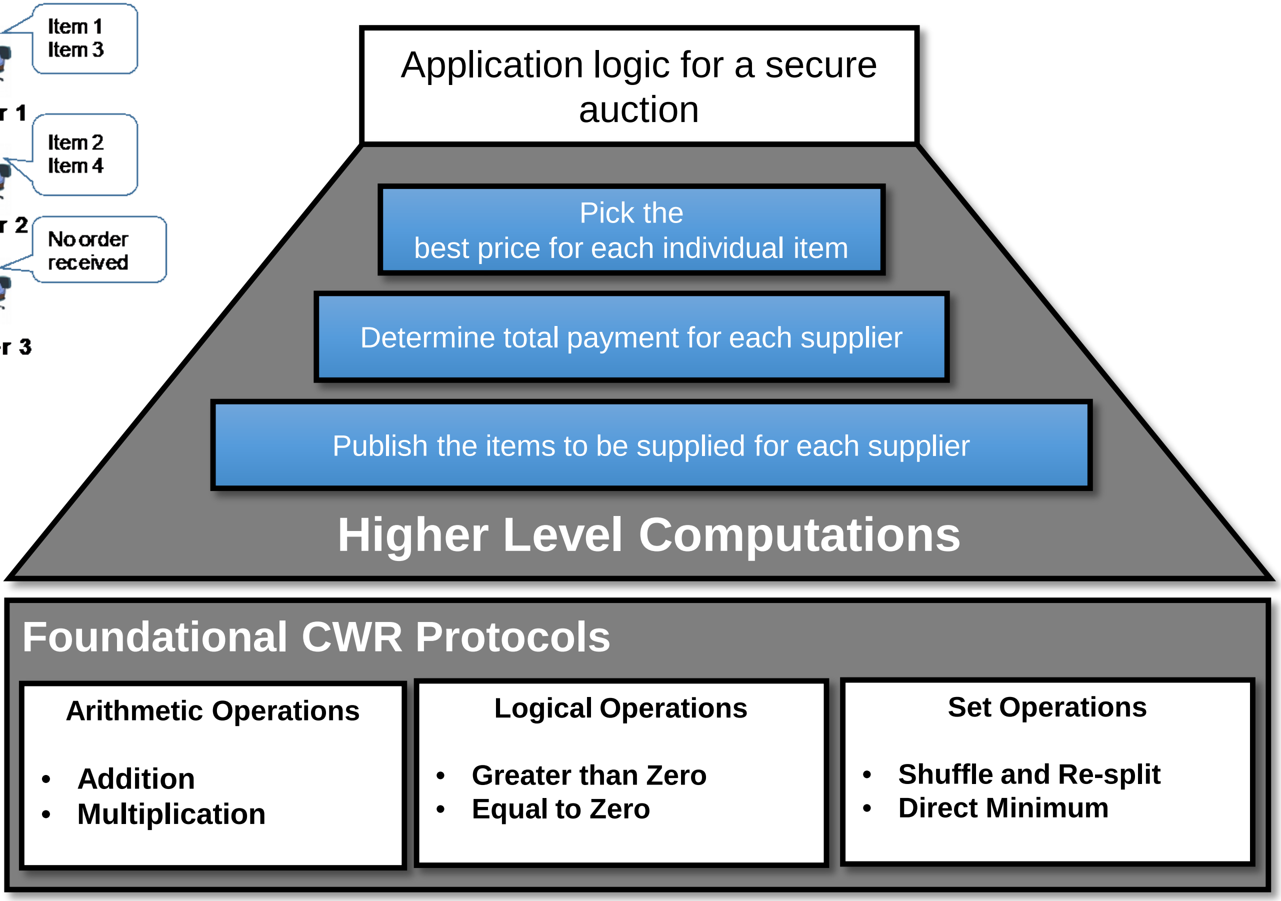
Logical Operations
- **Greater than Zero**
- **Equal to Zero**

Set Operations
- **Shuffle and Re-split**
- **Direct Minimum**

[1] Chaduvula, S.C. 2019. Secure Co-Design: Confidentiality Preservation in Online Engineering Collaborations. PhD Dissertation. Purdue University, West Lafayette, IN

CWR-based Secure Auctions





Application logic for a secure auction

Pick the best price for each individual item

Determine total payment for each supplier

Publish the items to be supplied for each supplier

Higher Level Computations

Foundational CWR Protocols

Arithmetic Operations

- **Addition**
- **Multiplication**

Logical Operations

- **Greater than Zero**
- **Equal to Zero**

Set Operations

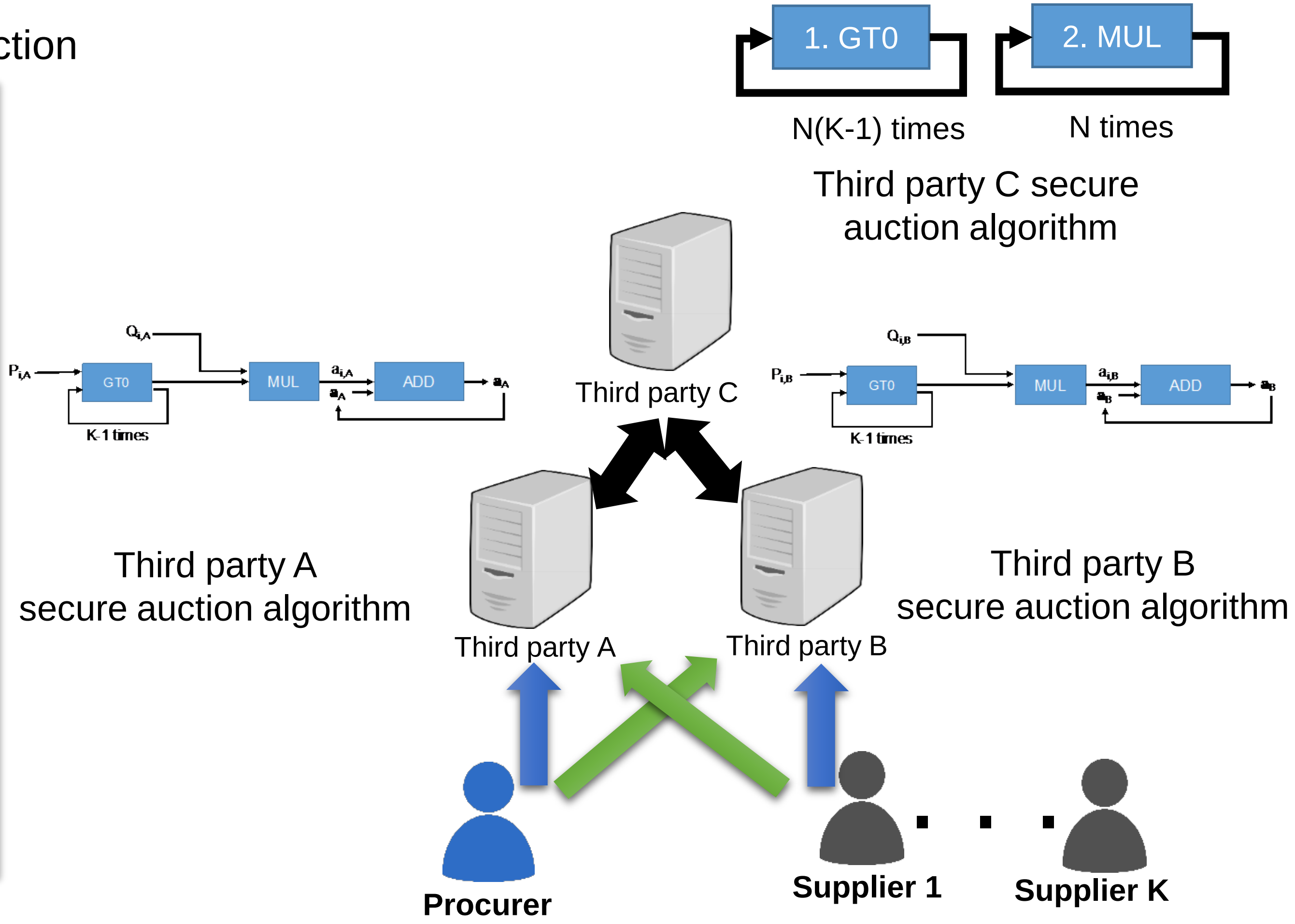
- **Shuffle and Re-split**
- **Direct Minimum**

CWR can be used to construct different types of auctions, including first-price and second-price

Architecture of CWR-based Secure Auctions

Pseudo-code for a secure auction

- For each item
  - Pick the lowest item price
  - Multiply the lowest item price with the respective quantity
  - Add the product to the payment corresponding to the winning supplier

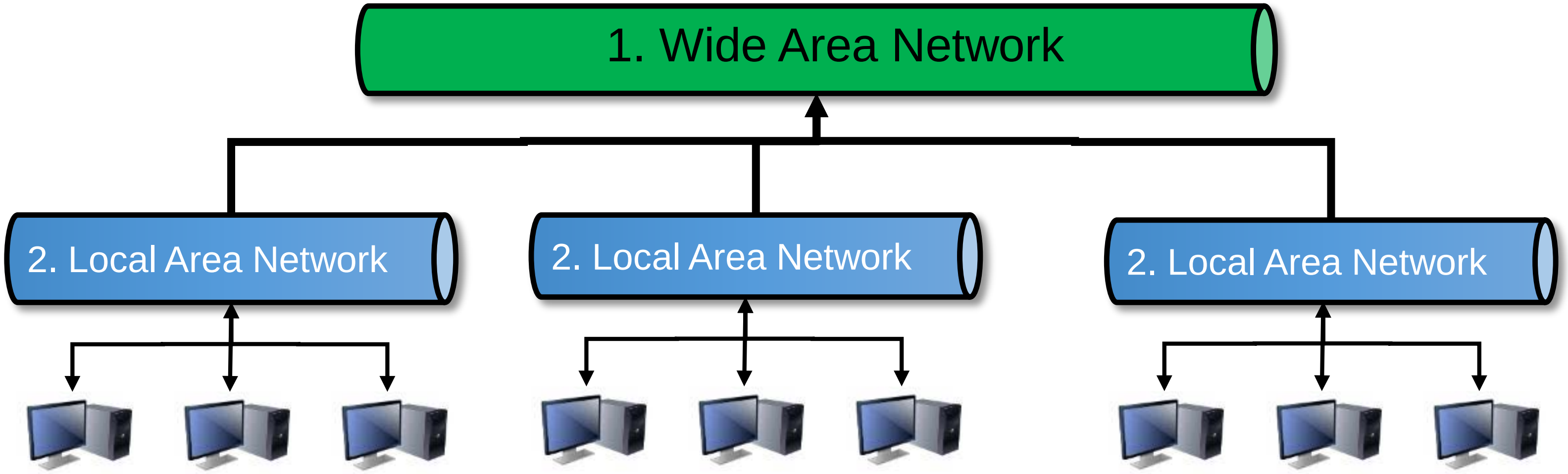


MUL→ Multiplication Protocol
ADD→ Addition Protocol
GT0 → Greater than Zero Protocol
sVIP→ Vector Inner Product Protocol

Procurer can "cherry pick" the best price for each item without requiring suppliers to disclose their bids for individual items

CWR Performance Evaluation

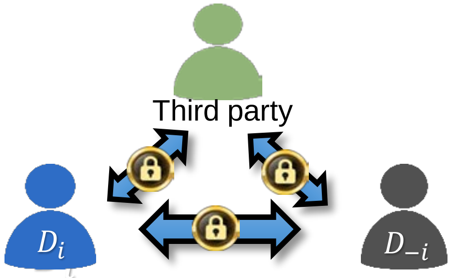
- Experimental Setup



- Key performance indicators
  - Total computation time (s)
  - Amount of data transferred (kB)

Results: Secure Vector Inner Product

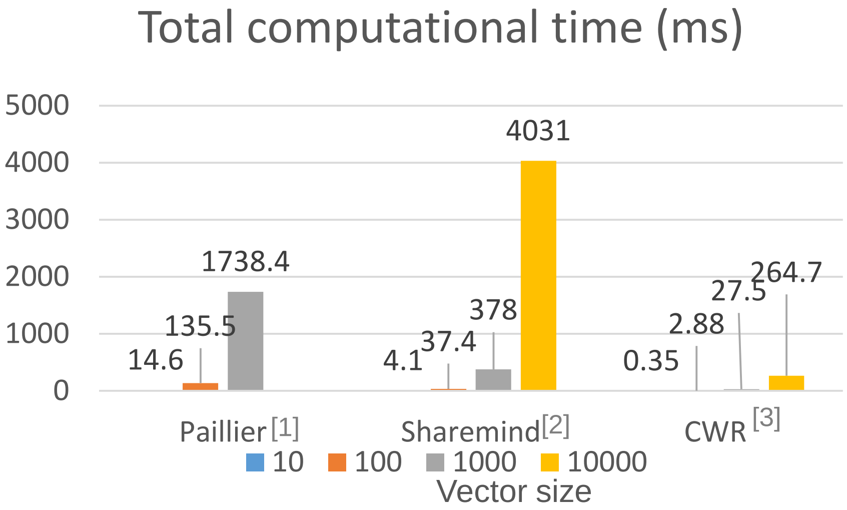
$$\boldsymbol{b} = \begin{bmatrix} b_1 \\ \vdots \\ b_n \end{bmatrix}$$

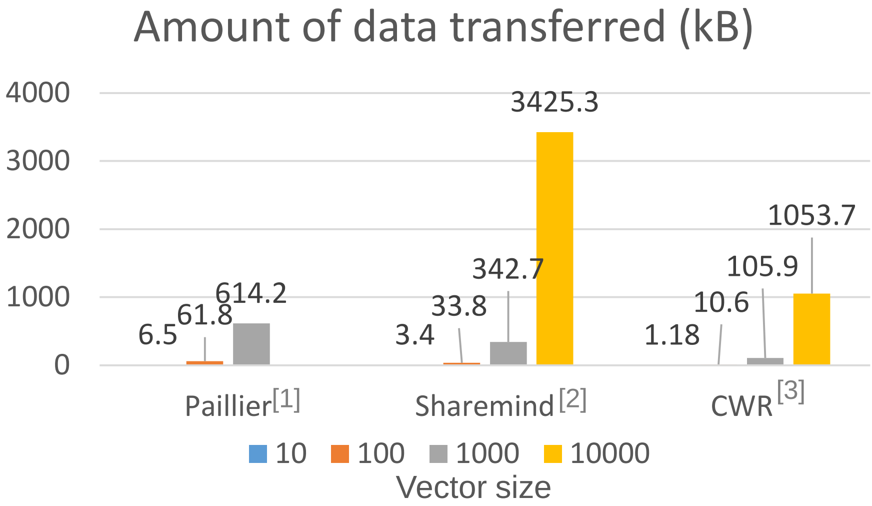


$$\mathbf{d} = \begin{bmatrix} d_1 \\ \vdots \\ d_n \end{bmatrix}$$

Confidential Input Vector: **b**
Output: k=**b.d**

Confidential Input Vector: **d**
Output: k=**b.d**





[1] Paillier, Pascal. "Public-key cryptosystems based on composite degree residuosity classes." In *Eurocrypt*, vol. 99, pp. 223-238. 1999.

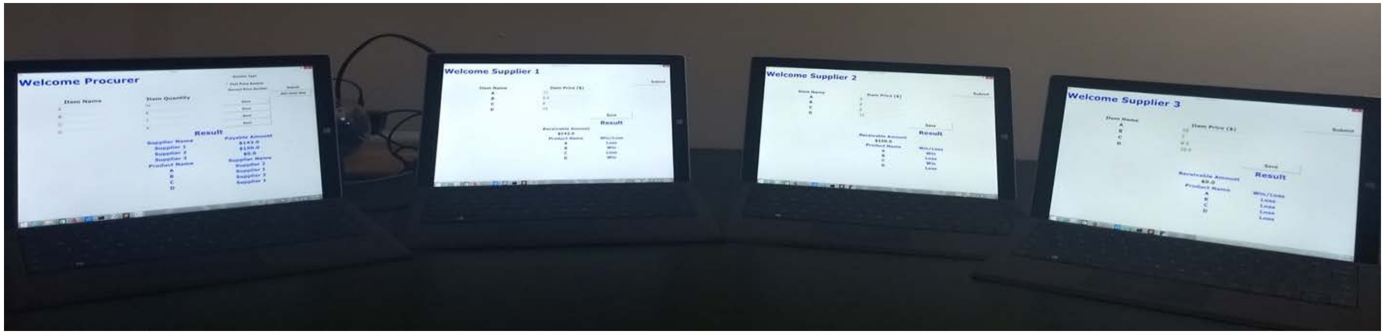
[2] Bogdanov, D., Niitsoo, M., Toft, T., & Willemson, J. (2012). High-performance secure multi-party computation for data mining applications. *International Journal of Information Security*, *11*(6), 403-418.

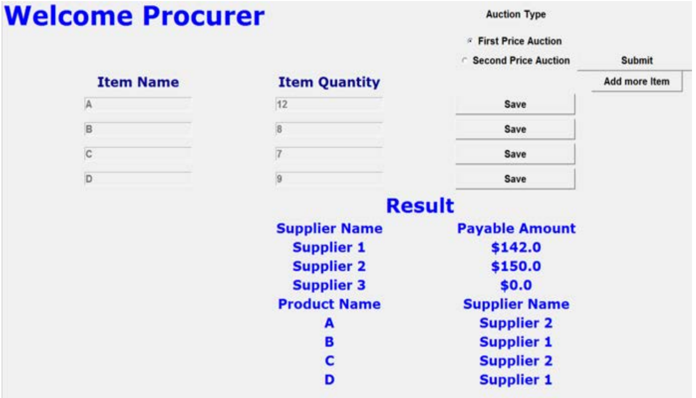
[3] Chaduvula, S.C., Panchal, J.H., and Atallah, M.J., 2019. Computing without Revealing: A Cryptographic Approach to eProcurement *Naval Post Graduate School*. Naval Postgraduate School, Monterey, CA 93943.

CWR-based inner product is computationally lightweight compared to competing techniques

Experimental Setup: CWR-based Secure Auctions

Item Name	Procurer (Quantity)	Supplier 1 (Item price)	Supplier 2 (Item price)	Supplier 3 (Item price)
A	12	$11	$9	$10
B	8	$6.5	$8	$7
C	7	$8	$6	$6.5
D	9	$10	$12	$10.5





Welcome Procurer

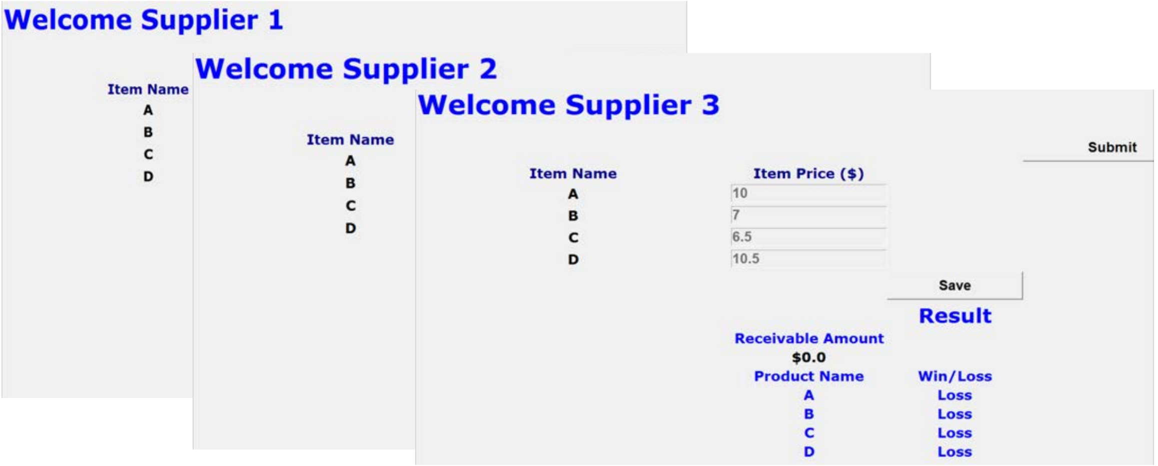
Auction Type

● First Price Auction
○ Second Price Auction

Item Name	Item Quantity		
			Submit
			Add more Item
A	12	Save	
B	8	Save	
C	7	Save	
D	9	Save	

Result

Supplier Name	Payable Amount
Supplier 1	$142.0
Supplier 2	$150.0
Supplier 3	$0.0
Product Name	**Supplier Name**
A	Supplier 2
B	Supplier 1
C	Supplier 2
D	Supplier 1



Welcome Supplier 1

Item Name
A
B
C
D

Welcome Supplier 2

Item Name
A
B
C
D

Welcome Supplier 3

Submit

Item Name	Item Price ($)
A	10
B	7
C	6.5
D	10.5

Save

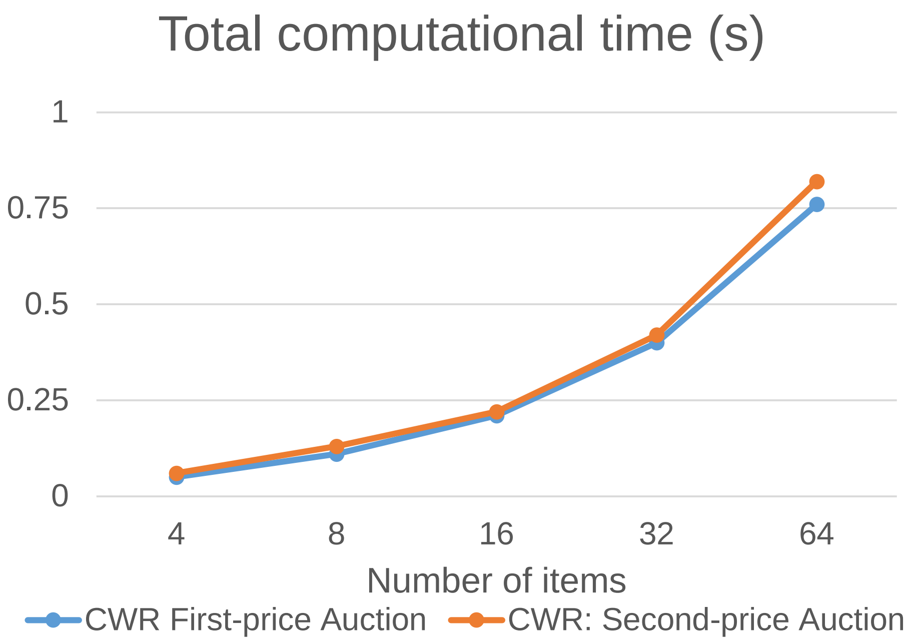
Result

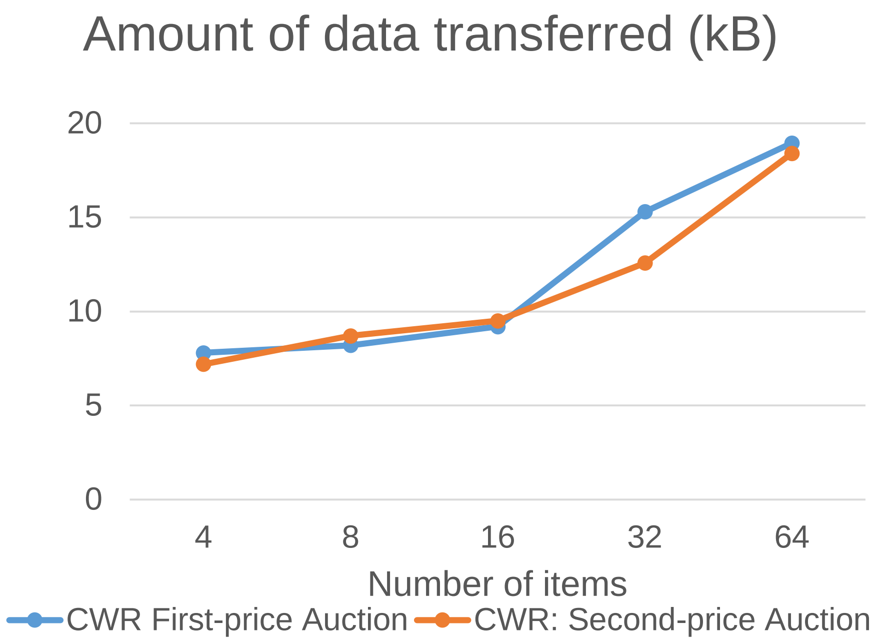
Receivable Amount
$0.0

Product Name	Win/Loss
A	Loss
B	Loss
C	Loss
D	Loss

CWR-based auctions enable procurers to “cherry-pick” the best price for each item

Results: CWR-based Secure Auctions[1]





# Test conditions: LAN with 2Mbps

[1] Chaduvula, S.C., Panchal, J.H., and Atallah, M.J., 2019. Computing without Revealing: A Cryptographic Approach to eProcurement *Naval Post Graduate School*. Naval Postgraduate School, Monterey, CA 93943.

CWR-based auctions are scalable

Summary

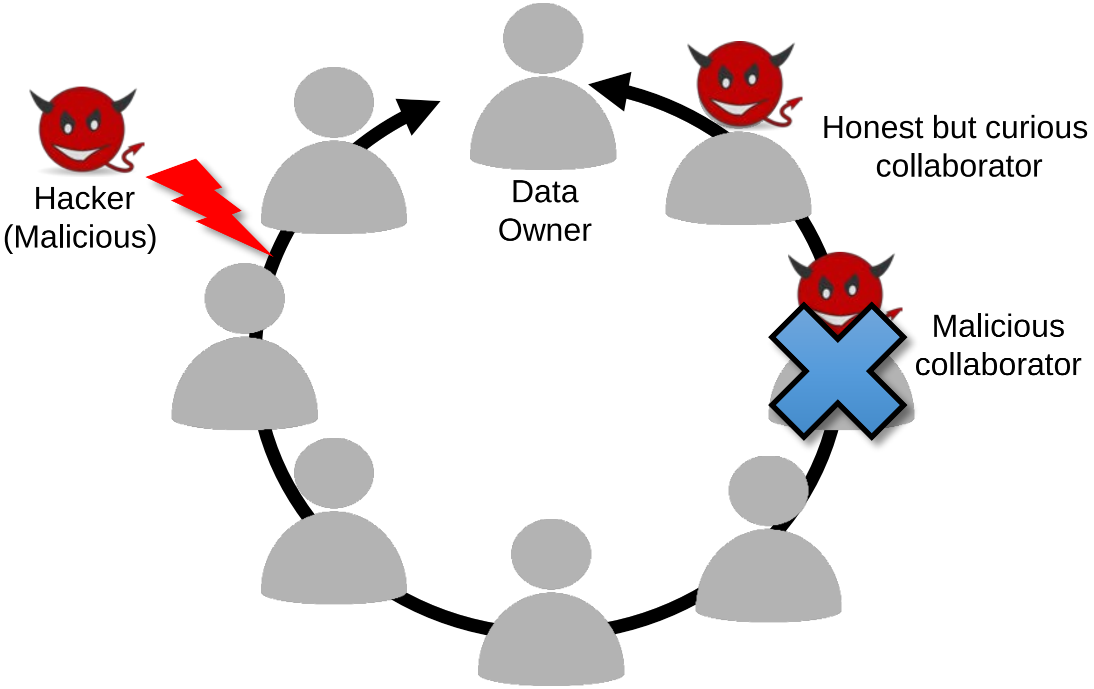
- **Advantages**
  - No abuse of confidential data (bids, etc.)
  - Computationally lightweight
  - No cryptographic key management
  - No specialized infrastructure required
  - Overcomes supplier vulnerabilities

- **Assumptions**
  - Procurers, suppliers and third parties are honest-but-curious
  - Suppliers and third parties do not collude
  - Procurer and suppliers mutually agree on the auction mechanism

THANK YOU!

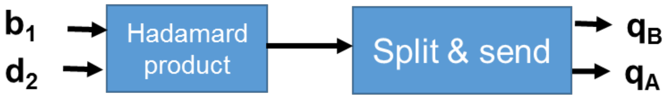
Backup

Limitations

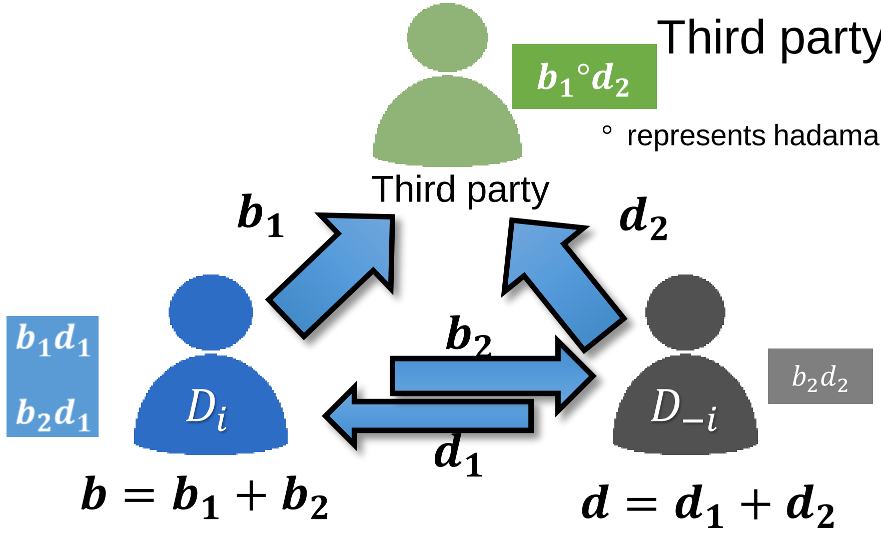


CWR fails against malicious collaborators

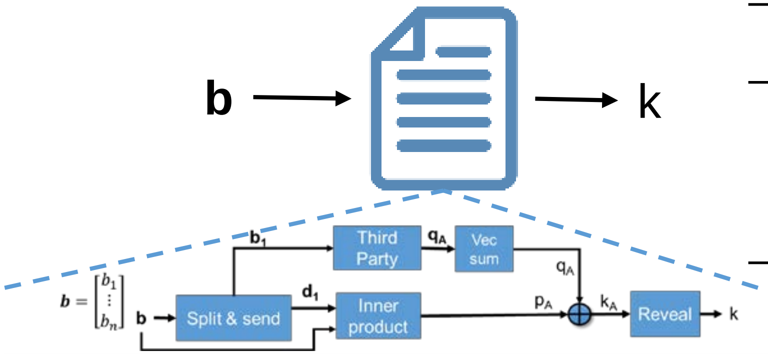
Modified sVIP protocol



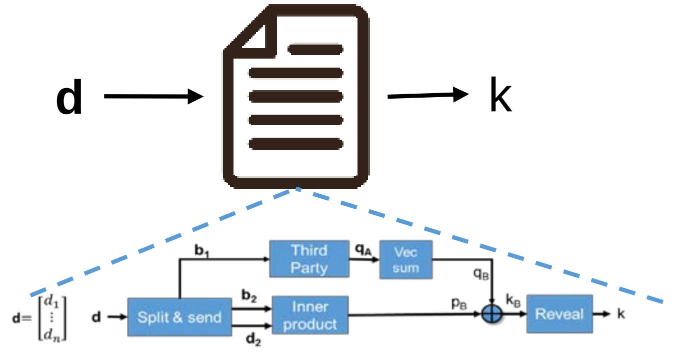
Third party's sVIP algorithm



∘ represents hadamard product



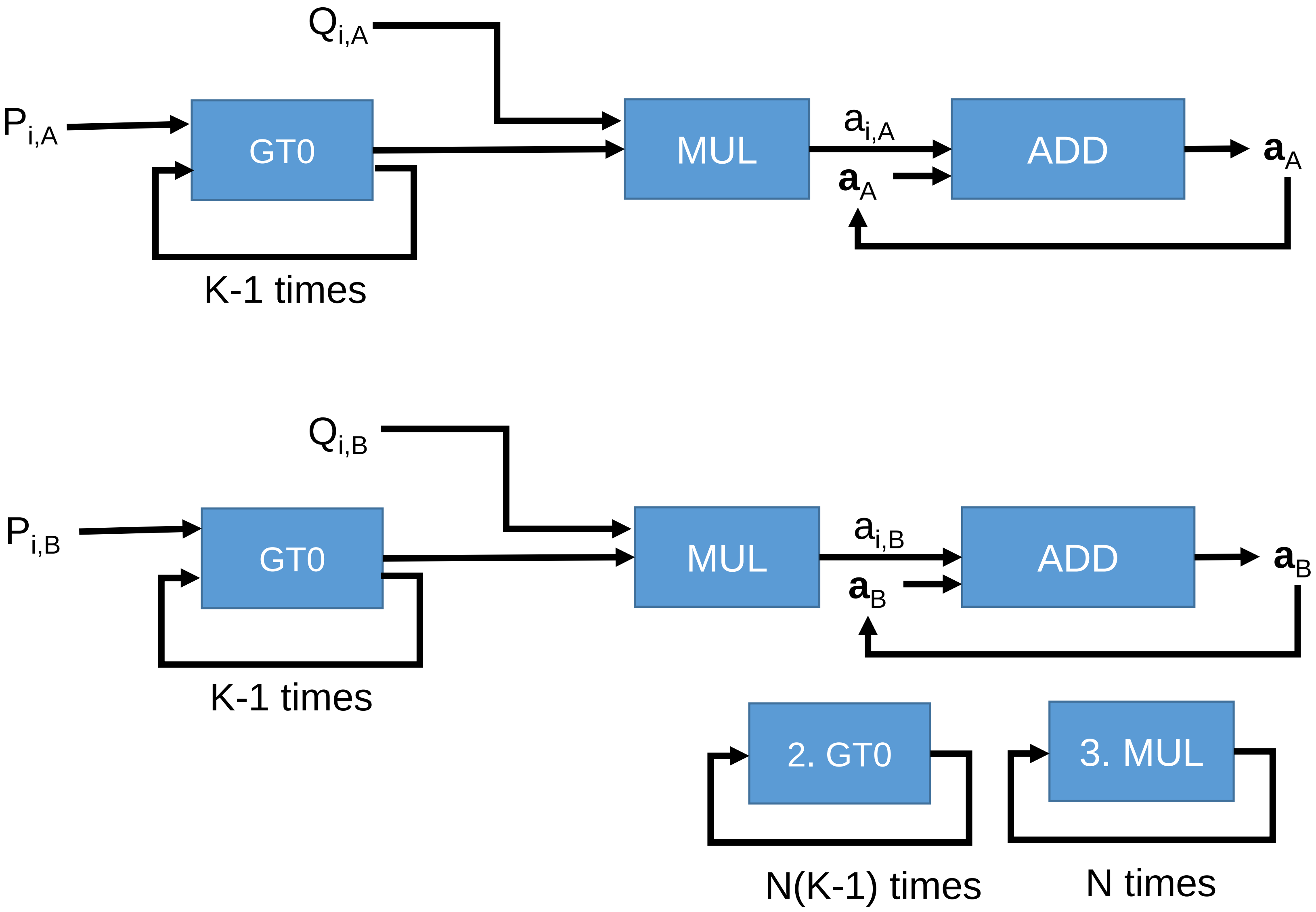
b.d	d_1	d_2
b_1	$b_1 d_1$	$b_1 d_2$
b_2	$b_2 d_1$	$b_2 d_2$



Modified sVIP protocol hides not only values but also nature of computation from the third party

Future Work

- Expand CWR-based secure auctions to volume-based pricing
- Secure handling of payments



$Q_{i,A}$

$P_{i,A}$

GT0

MUL

$a_{i,A}$

ADD

$\mathbf{a}_A$

$\mathbf{a}_A$

K-1 times

$Q_{i,B}$

$P_{i,B}$

GT0

MUL

$a_{i,B}$

ADD

$\mathbf{a}_B$

$\mathbf{a}_B$

K-1 times

2. GT0

3. MUL

N(K-1) times

N times