SYM-AM-19-043

PROCEEDINGS
OF THE
SIXTEENTH ANNUAL ACQUISITION RESEARCH SYMPOSIUM

WEDNESDAY SESSIONS
VOLUME I

Acquisition Research:
Creating Synergy for Informed Change

May 8–9, 2019

Published: April 30, 2019

Prepared for the Naval Postgraduate School, Monterey, CA 93943.

ACQUISITION RESEARCH PROGRAM
GRADUATE SCHOOL OF BUSINESS & PUBLIC POLICY
NAVAL POSTGRADUATE SCHOOL

Computing Without Revealing: A Cryptographic Approach to eProcurement

Siva C Chaduvula—is a PhD student at Purdue University. His research interests are in cryptography, machine learning, and design. Prior to his PhD, he worked as a Deputy Manager at Bosch Limited. He completed his bachelor's and master's from Indian Institute of Technology Madras (IITM), Chennai, India.

Jitesh H. Panchal—is an Associate Professor in the School of Mechanical Engineering at Purdue University. He received his BTech (2000) from Indian Institute of Technology (IIT) Guwahati, and MS (2003) and PhD (2005) in mechanical engineering from Georgia Institute of Technology. Panchal's research interests are in the science of systems engineering with focus on three areas: democratization of design and manufacturing, decision making in decentralized socio-technical systems, and integrated products and materials design. He is a co-author of the book *Integrated Design of Multiscale, Multifunctional Materials and Products*. He is a recipient of the CAREER award from the National Science Foundation (NSF), the Young Engineer Award and two best paper awards from ASME CIE division, and a university silver medal from IIT Guwahati.

Mikhail J. Atallah—has research interests in information security and algorithms. His work on key management received the 2015 CCS Test of Time Award. He was the 2017 recipient of the Purdue Arden L. Bement, Jr. Award, the most prestigious award the university bestows in pure and applied science and engineering. He was the 2016 recipient of the Purdue Sigma Xi Faculty Research Award and the 2013 recipient of the Purdue Outstanding Commercialization Award. He is a Fellow of both the ACM and IEEE, and was a speaker nine times in the Distinguished Lecture Series of top computer science departments. Atallah has been the keynote and invited speaker at many national and international meetings and has served on the editorial boards of top journals and on the program committees of top conferences and workshops. He was selected in 1999 as one of the best teachers in the history of Purdue University and included in Purdue's Book of Great Teachers, a permanent wall display of Purdue's best teachers past and present. In 2001, he co-founded Arxan Technologies Inc to commercialize a software protection technology developed jointly with his doctoral student Hoi Chang. (In October 2015, Arxan reported that applications secured by it were running on more than 500 million devices.) He was CTO of Arxan Technologies and Chief Scientist for its defense subsidiary, Arxan Defense Systems. Arxan Defense Systems was acquired in 2010 by Microsemi Corporation, and Arxan Technologies was acquired in 2013 by the private equity firm TA Associates.

Abstract

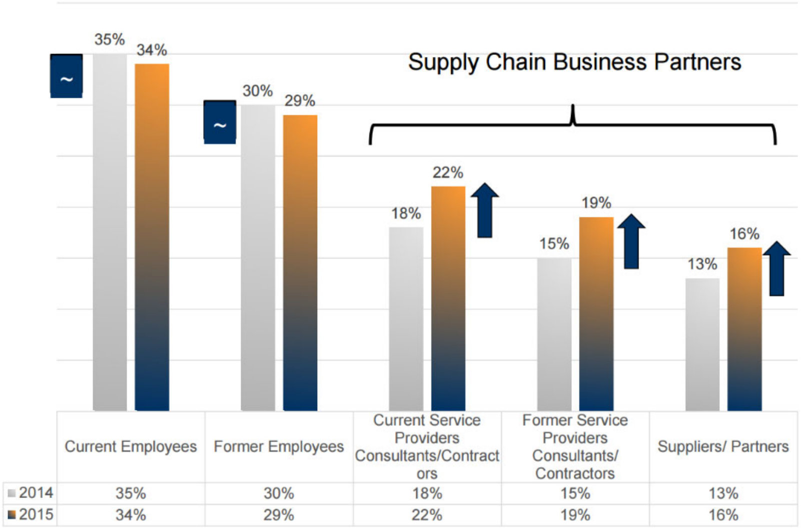
In typical eProcurement processes, sensitive data such as prices, intellectual property, and customer information often flow across enterprise boundaries. Such data sharing amplifies the risk of a data breach due to exposure to the potential security flaws of prospective and current eProcurement partners. Threats of information leakage inhibit enterprises from sharing sensitive data; thus, enterprises cannot take full advantage of the eProcurement process. Existing cryptography-based data sharing protocols impose a high computational burden for maintaining data confidentiality, making them unsuitable for real-time applications such as eProcurement. With this motivation, we address the following research question: How can procurers and suppliers securely conduct their business transactions without revealing their confidential information?

The proposed approach enables procurers and suppliers to perform computations while preserving their confidential data. In this paper, we show how Computing-Without-Revealing (CWR)–based data sharing protocols can be used as building blocks to execute procurement auctions for standard products. A web-based platform is developed to measure the performance of the CWR protocols against competing techniques. Experimental results corroborate the efficiency of the CWR-based protocols, making them suitable for real-time

applications. The application of the protocols is demonstrated for different eProcurement scenarios, including first- and second-price auctions for standard products.

Introduction

The design and manufacturing of products, regardless of complexity, involve partnerships with third-party vendors, manufacturers, suppliers, contractors, and other entities outside the organization. The design of a Boeing 777 airplane, for example, involved more than 10,000 people external to Boeing. Similarly, Ford Motor Company works with more than 1,000 suppliers across the globe. Such partnerships allow organizations to focus on their core expertise, thereby increasing their effectiveness. However, there are also risks associated with sharing confidential information with business partners. In the 2016 acquisition research symposium, it was highlighted that business partners pose a significant malicious threat because they are a part of the information flow (see Figure 1). Therefore, there is a growing need for research and development on technologies that enable business transactions without revealing confidential information of the participants.



	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,*

Figure 1. Incidents of Data Breaches Among Business Partners
(Kaestner, Arndt, & Dillon-Merrill, 2016)

Traditionally, business transactions between a procurer and suppliers involve a trusted third party (TTP), such as a cloud service provider. The procurer and suppliers send their confidential information to a TTP, who performs the required computation. Although this is easy to implement, the main risk is that rogue employees of the TTP (e.g., the people who maintain and update cloud servers) can learn the confidential information. Additionally, information may be compromised through a break-in by hackers, through a malware or spyware infestation, or even in a completely non-malicious (i.e., accidental) manner. There is also a potential risk that the cloud service provider may, as an organization, decide to betray the users by revealing or secretly using their confidential inputs. A recent report (Ponemon, 2018) highlighted the impact of internal attacks by insiders/contractors on organizations (see Figure 2). Therefore, it is important to preserve the confidentiality of an organization's data while engaging with current and especially potential suppliers.

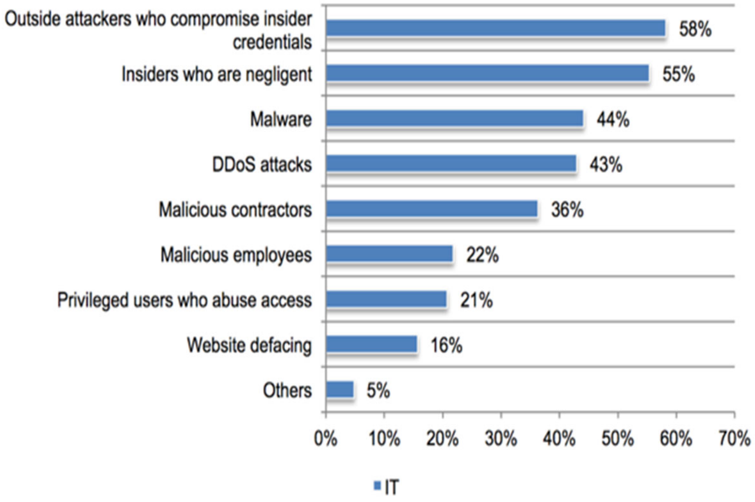


Figure 2. Influence of Different Security Threats Faced by Organizations
(Ponemon, 2018)

In a typical eProcurement process, sensitive information related to prices, intellectual property, and customer data often flow across enterprise boundaries. While this data flow between eProcurement partners is important for performing business operations, there exist data security concerns, especially when the data involves intellectual property, trade secrets, etc. Sharing such confidential data amplifies the risk of data breach due to potential security flaws of the partners in the eProcurement process. Such threats discourage enterprises from sharing sensitive data, and thus prevents them from taking full advantage of the eProcurement process.

In this paper, we present an approach for addressing this fundamental challenge. The approach enables secure eProcurement of standard products. We present the use of cryptographic protocols to execute auction mechanisms within an eProcurement process, where the procurer only learns confidential information related to winning bidders. No confidential information about the losing bidders is revealed to anyone, including the procurer, thereby resulting in truthful revelation and increasing value for all participants involved. This proposed eProcurement process promises economic advantages for a wide variety of private-sector organizations ranging from large electronics manufacturers and automakers to small and medium-sized enterprises specializing in specific technologies.

Overview of the Approach

Current procurement processes are characterized by incomplete and disaggregated information about (i) the capabilities and cost structure of individual suppliers and (ii) the requirements of the procurers. In a typical eProcurement process, such as a sealed-bid reverse auction, as shown in Figure 3, procurement happens in three stages. In Stage 1, the procurer reveals his/her requirements to the suppliers. In Stage 2, suppliers submit their consolidated bids. In Stage 3, the procurer analyzes the submissions and determines the winner by choosing the supplier with the best technology at the lowest bidding price.

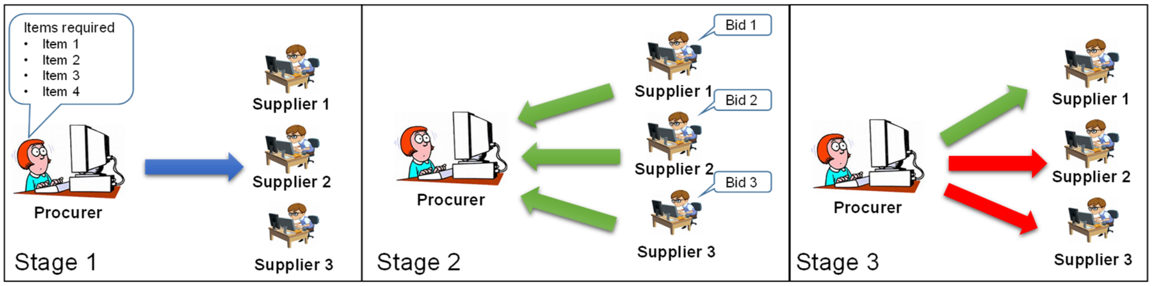


Figure 3. Existing Approach for Sealed-Bid Auctions

In such a setting, suppliers would ideally like the procurer to learn their confidential cost information and the details of the proprietary technology only if they win the contract. However, procurers need to determine the quality and suitability of the technology to choose the winner. In addition, procurers may not want to reveal their requirements, especially if the requirements reveal their competitive advantage. This reluctance to reveal sensitive information may drive the procurer to settle for inferior solutions, thereby reducing the overall effectiveness of the procurement mechanism. This brings us to the research question addressed in this study: How can procurers and suppliers securely conduct their business transactions without revealing their confidential information?

Our central hypothesis for this project is that the fundamental protocols discussed in the Details of the Technical Approach section can be used as building blocks to perform the computations involved in an eProcurement process. Computational results derived using Computing-Without-Revealing (CWR) protocols help in reducing information asymmetry while also protecting the sensitive information held by procurers and suppliers. Such an approach enables procurers and suppliers to estimate the challenges and uncertainties involved and thereby help both sides of the eProcurement process in making informed decisions.

Procurement processes based on the proposed CWR approach enjoy the following benefits:

- **No cryptographic key management:** No data is lost if the secret key used for determining the splits is inadvertently lost.
- **Computation time:** The proposed protocols are computationally lightweight, unlike homomorphic encryption and circuit evaluation. Hence, it is possible to perform huge computations with weaker and battery-powered portable devices such as smart phones.
- **No data abuse:** The data is handled by cloud servers, procurers, and suppliers. No user learns the actual inputs of their counterparts. Hence, there is no possibility of misusing the data. Even if there is a breach in one of the cloud servers, the data that a hacker can access would only be a share of the actual data.
- **No specialized infrastructure required:** Since their confidential information is protected, procurers and suppliers can use commercial cloud services for procurement processes. This has cost advantages in terms of capital expenditure and IT expenses.
- **Overcomes supplier vulnerabilities:** The procurer need not worry about a data breach at the supplier's end as the data breached (if any) at the vendor's end will

be only a share of the actual data. Therefore, no meaningful data would be leaked.

A sub-field within cryptography, called “secure multi-party computations” (SMC), focuses on enabling multiple parties to jointly process their individual confidential data into useful information while preserving the confidentiality of the data belonging to each party. Existing cryptographic practices to perform computations securely can be classified into two broad categories:

1. **No Need of a Third Party:** Cryptographic techniques such as fully homomorphic encryption (Bogetoft et al., 2009), secure circuit evaluation [Ben-David, Nisan, & Pinkas, 2008), and partial homomorphic encryption (PHE; Paillier, 1999) use encryption-based techniques to hide confidential data. Encrypted data is exchanged between parties and computations are performed on the exchanged encrypted data. Such computations impose a very high computational burden and the times reported using these techniques are much longer than in the case of the traditional TTP approach, which makes them ill-suited for use in practical scenarios.
2. **No Need to Reveal to the Third Party:** On the other hand, using secret sharing techniques is a way to distribute a secret (or confidential data) among a group of parties, where every party is allocated a share of the secret. This secret can be reconstructed only when a sufficient number of shares are combined. Individual shares do not infer anything about the whole secret.

Secret sharing approaches are comparatively faster than encryption-based approaches. The approach proposed in this study reduces the computational burden, which makes it easier to adapt. Moreover, as the proposed approach is based on general arithmetic primitives, it is well suited for quickly building secure collaborative computing platforms for new procurement scenarios or for variants of the current state of practice, such as volume-based pricing, which is not handled in previous work.

Details of the Technical Approach

EProcurement involves standard processes such as request for proposals (RFPs), auctions, payments, etc. Usually, these processes require inputs from both procurers and suppliers. We present a secure multi-party computation (SMC) technique that allows procurers and suppliers to perform the computations involved in these standard processes without needing to reveal their confidential inputs to anyone. We term our approach of the SMC technique as Computing-Without-Revealing (CWR). It builds on the protocols developed by the PIs, which are presented in Wang et al. (2017). The approach is based on two key principles (Wang et al., 2013):

- Adding/multiplying an input with a random number hides the value of the input. If the random number is much larger than the input, it also hides the order of magnitude.
- Adding/multiplying with a large number is orders of magnitude faster than the use of expensive cryptographic techniques such as homomorphic encryption and secure circuit evaluation.

Consider a scenario where the confidential value is 11. We additively split the value into random-looking shares and a participating cloud server sees only one of the random-looking shares. For example, the additive splits of 11 could be 1819 and –1808 (see Figure 4); it could just as well have been 103 and –92 or –19 and 30. These additively split values of 11 are stored in two different cloud servers. We developed protocols for basic arithmetic operations on such additive splits (see Wang et al., 2017, for details).

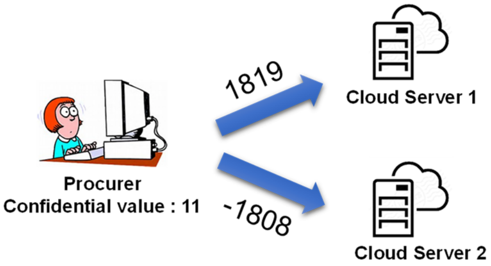


Figure 4. Additive Splits

The CWR approach utilizes these splits to perform the desired computation without revealing the input data to anyone. In the next section, we review the structure of the CWR protocols.

Foundational Computing-Without-Revealing (CWR) Protocols

CWR protocols enable a procurer (referred to as Alice) and suppliers (referred to as Bob) to use a single external server (referred to as Helper) to perform the computations that are mutually agreed upon between Alice and Bob. The following is the generalized structure of the CWR protocols:

- **Stage 1—Pre-processing of inputs.** The pre-processing of inputs involves two steps:

  (a) Split the inputs additively if the inputs from Alice/Bob are not additive splits.

  (b) Alice/Bob agree on a morphing function and a distribution from which random numbers are generated. Alice/Bob morph the additive splits using this morphing function and random numbers from the distribution. These morphed additive splits prevent the Helper from learning about Alice/Bob when shared with the Helper.

- **Stage 2—Run the desired computations securely.** Alice/Bob derive the application logic from their mutually agreed computation. Alice/Bob provide the application logic along with the morphed additive splits to the Helper. The application logic involves the sequence of computations that need to be performed on the morphed additive splits. The output derived from running the application logic is additively split. One of the additive splits corresponding to the output is shared with Alice and the other with Bob.

- **Stage 3—Post processing of outputs.** Alice and Bob post-process their additive splits before sharing them with each other. Alice and Bob simultaneously exchange the processed outputs with each other. Alice and Bob independently add their additive splits and learn the actual output of the computation.

Using this structure, CWR protocols for fundamental mathematical operations are proposed (Wang et al., 2017). In the rest of this paper, we denote CWR-MP to denote multiplication protocol and CWR-GT0 to denote greater than zero protocol within the CWR setting. These foundational protocols are used as building blocks to construct protocols for higher level mathematical calculations. In the next section, we discuss how these protocols can be extended to eProcurement.

Extension of CWR to eProcurement

In this paper, we present a procurement platform that enables participants of a procurement process to execute the computations involved using CWR technology. Specifically, we focused on an auction platform for standard products. However, this approach can be extended to different types of auctions suited for their business needs.

In the following sections, we describe these CWR-based auction platforms in a greater detail.

Extension of CWR to Auctions for Standard Products

In this section, we assume that standard products or commercial-off-the-shelf items are those items where the quality of these products is established. So, the decision on the auction winner is based on the price of the product.

While there are many ways to perform auctions within an eProcurement process for standard products, in what follows, we use reverse sealed-bid auctions to illustrate how CWR protocols can be used as building blocks to perform the computations involved (as shown in Figure 4). Note that the CWR-protocols can be constructed to perform the computations involved in any auction mechanism, but to simplify the discussion, we focus on the first price reverse sealed-bid auction. The computation involved in such auctions is the identification of a supplier with the minimum consolidated bid for all the items listed by the procurer. The procurer and suppliers mutually agree on three external servers (for example, cloud servers $\alpha, \beta, \text{and } \gamma$). The procurer provides unique IDs to all the suppliers. Suppliers share the additive splits corresponding to their confidential information (i.e., consolidated bids) along with their IDs with cloud server α and cloud server β. Cloud server α (as Alice) and cloud server β (as Bob), together with cloud server γ (as Helper), deploy Protocol 1. After Protocol 1 ends, the cloud servers $\alpha \text{ and } \beta$ share the additive splits obtained with the procurer. By adding these additive splits, the procurer finds the supplier with the minimum consolidated bid and the value of the consolidated bid.

This extension of CWR to eProcurement enables procurers and suppliers to perform procurement transactions without needing to reveal their confidential information to anyone. This allows procurers to design auction mechanisms that can help them overcome inefficiencies in existing auction mechanisms. For example, an auction mechanism built using CWR can identify the supplier with the best price (i.e., “cherry pick” the suppliers) for each and every item. Such an auction mechanism has great potential to reduce procurement costs, as the procurer gets the best possible price for every item. This will appeal to suppliers as well because their individual item prices are not revealed to anyone, including to the procurer. In this section, we present a CWR first price reverse auction that enables the procurer to select the supplier who provides the greatest bang for their buck for each individual item and thereby overcome this inefficiency.

CWR First Price Reverse Auction

In a CWR first price reverse auction, a single procurer (say, the DoD) can “cherry pick” the best supplier among the suppliers (DoD contractors) for each and every item. Figure 5 illustrates a scenario of CWR first price reverse auction. The CWR first price reverse auction is listed in Protocol 1.

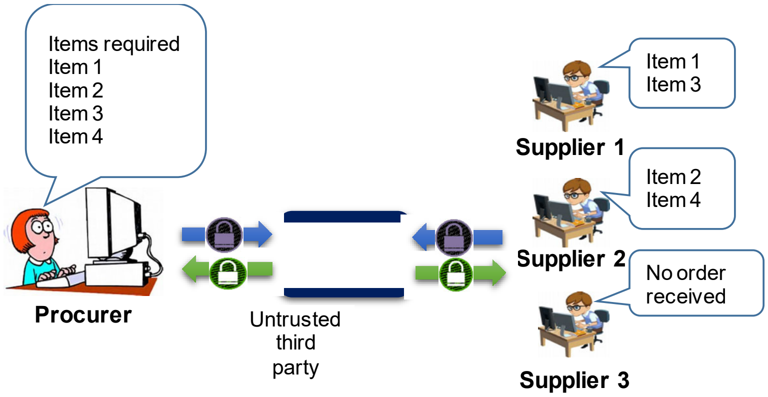


Figure 5. CWR-First Price Reverse Auction

The CWR first price reverse auction enables the procurer to learn only the payments that need to be made to each individual supplier and the items provided by each supplier. Throughout the protocol, the procurer cannot learn the supplier's individual item prices. Similarly, the supplier cannot learn the quantity desired by the procurer before the auction. The novelty in this protocol is that the external servers (cloud servers $\alpha, \beta, \text{and } \gamma$) on which the CWR protocols are run do not know the auction's context (item names, etc.) as they receive morphed additive splits. Therefore, the external servers learn nothing about the procurer's/supplier's confidential information. Note that this protocol is designed to choose the supplier based on a single attribute of the product (price). This protocol can be extended to multiple attributes with the appropriate weights.

Implementation Details

Below are some of the details for implementing the CWR first price reverse auction:

1. **Secure Channels:** It is important to understand that information exchanges that occur between parties within the CWR auction should use secure channels, such as HTTPS.
2. **Cross Accounts:** The ownership of the cloud server account is one of the concerns while deploying CWR. Existing cloud servers, such as Amazon Web Services (AWS), offer features such as cross accounts through which a procurer and suppliers can examine what algorithms are being run on their data splits. Please refer the following webpage for more details: https://docs.aws.amazon.com/IAM/latest/UserGuide/tutorial_cross-account-with-roles.html
3. **Tie Breaks:** There is a possibility that the item prices of suppliers may be the same. In such scenarios, the procurer can break such ties in many ways, including randomly picking a supplier from the suppliers with the same item price. How such ties are handled is made public to all participants prior to the auction.
4. **Single Item Winner:** In some scenarios, a supplier may win only one item. This can reveal the item price to the procurer when he/she makes payments. In such scenarios, the corresponding supplier is informed and the supplier may choose to participate/quit the procurement process.

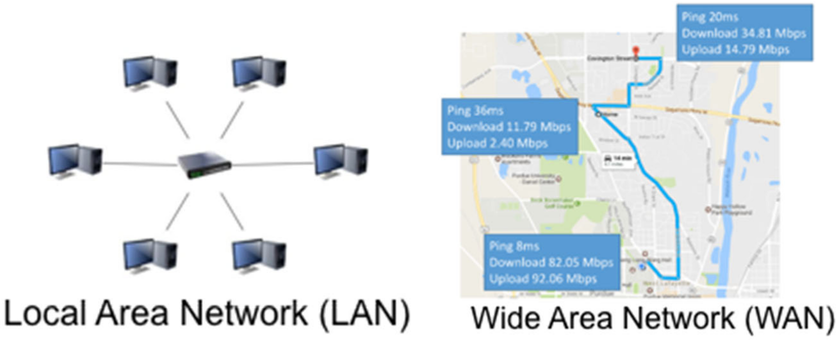
In the next section, we compare the performance of CWR-based computing techniques with competing secure computing techniques.

Performance Analysis of CWR

We developed a test-bench to run and compare different secure computing techniques such as partial homomorphic encryption and secret sharing, as discussed in the Overview of the Approach section. In what follows, we describe the test bed developed as part of this project to compare our approach (CWR) with the existing cryptographic approaches.

Test Bed Setup

We conducted experiments in two different settings. The first set of experiments was conducted when all the procurers and suppliers were connected to the same network (i.e., local area network or LAN). The second set of experiments was conducted when the procurers and suppliers were connected to different networks (i.e., wide area network or WAN). Note that the computation speed of all the approaches reduces with WAN. This is mainly attributed to the network latency.



Local Area Network (LAN)

Wide Area Network (WAN)

Figure 6. Experimental Setup

We identified computational time and bandwidth with respect to the amount of data that needs to be transferred between the procurer/suppliers as the key performance indicators (KPIs). The computational time is measured using a python module named "time" and the bandwidth is measured using an open source packet analyzer (Wireshark). We compared CWR protocols with competing secure computing techniques using these KPIs.

CWR-VIP

We chose the inner product as the computation to compare the performance of the proposed approach (CWR) against the existing approaches. This computation was chosen as it is commonly used to multiply the vector of quantity with the vector of item prices for the listed items within a procurement process.

We found that the proposed approach (CWR) is at least 10 times faster than the best existing approach (refer to Table 1) using LAN. We found that our approach is about 7 times faster than the best existing approach (see Table 2) using WAN. We realized that the cost of security (computational burden to maintain the confidentiality) in procurement activities is high (about 6–7 times) compared to open sharing, where procurement data is revealed to every participant. One of the reasons for this additional burden is the requirement of performing every computation using CWR protocols.

Table 1. Protocol Execution Time While Using LAN (in Seconds)

Vector length	0-server (PHE)	3-servers (Previous best) [9]	1-server (CWR-VIP)
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

Table 2. Protocol Execution Time While Using WAN (in Seconds)

Vector length	0-server (PHE)	3-servers (Previous best) [9]	1-server (CWR-VIP)
10	16.5	5.58	0.68
100	235	47.3	6.9
1000	>3600	486.3	74.7
10000	>3600	5567	742.6

In network communication, the amount of data (bandwidth) being exchanged between parties is another important performance indicator. In our comparative study, we found that our approach requires 3 times less bandwidth (refer to Table 3). These results indicate that our approach can be deployed in real-time applications and can be supported by devices with limited battery power.

Table 3. Comparison of Bandwidth Use (in KB)

Vector length	0-server (PHE)	3-servers (Previous best) [9]	1-server (CWR-VIP)
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

CWR-First Price Reverse Auction

We developed the software embodiment of the CWR-first price reverse auction (described in Protocol 1) and used it as an auction mechanism in a procurement process.

We used the values shown in Table 4 to simulate the auction mechanism. In what follows, we describe the outcomes of a traditional sealed bid auction and compare these outcomes with those obtained using CWR-first price reverse auction.

In a traditional sealed-bid auction, the procurer reveals the desired quantity. The suppliers submit their respective sealed bids ($330, $322, $316) to the procurer, who selects the minimum bid ($316) in first price auction and receives the items from Supplier 3. Throughout the auction process, suppliers hide their item prices in the form of sealed bids. However, from Table 4, we learn that Supplier 3 does not provide the best prices for each individual item.

Table 4. Item Prices and Quantities Used for Simulation Studies

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

Figure 7 shows a picture of the demo of this CWR-first price reverse auction, developed as part of this project. In this demo, one Microsoft SurfacePro computer was used as the procurer and three other SurfacePros were used as the suppliers to simulate a reverse auction. All the surface pros were connected with each other using 2 Mbps (upload/download speed) LAN. The procurer and suppliers mutually agree on three external servers ($\alpha, \beta, \text{and } \gamma$) which are used to run the CWR first price reverse auction. A computer is used to run these three external servers and this computer is also connected to all the SurfacePros using the same LAN.

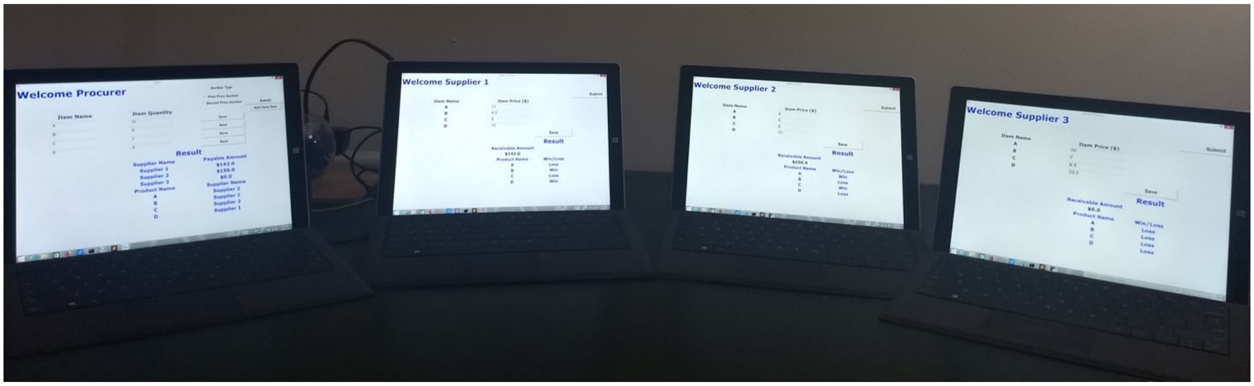
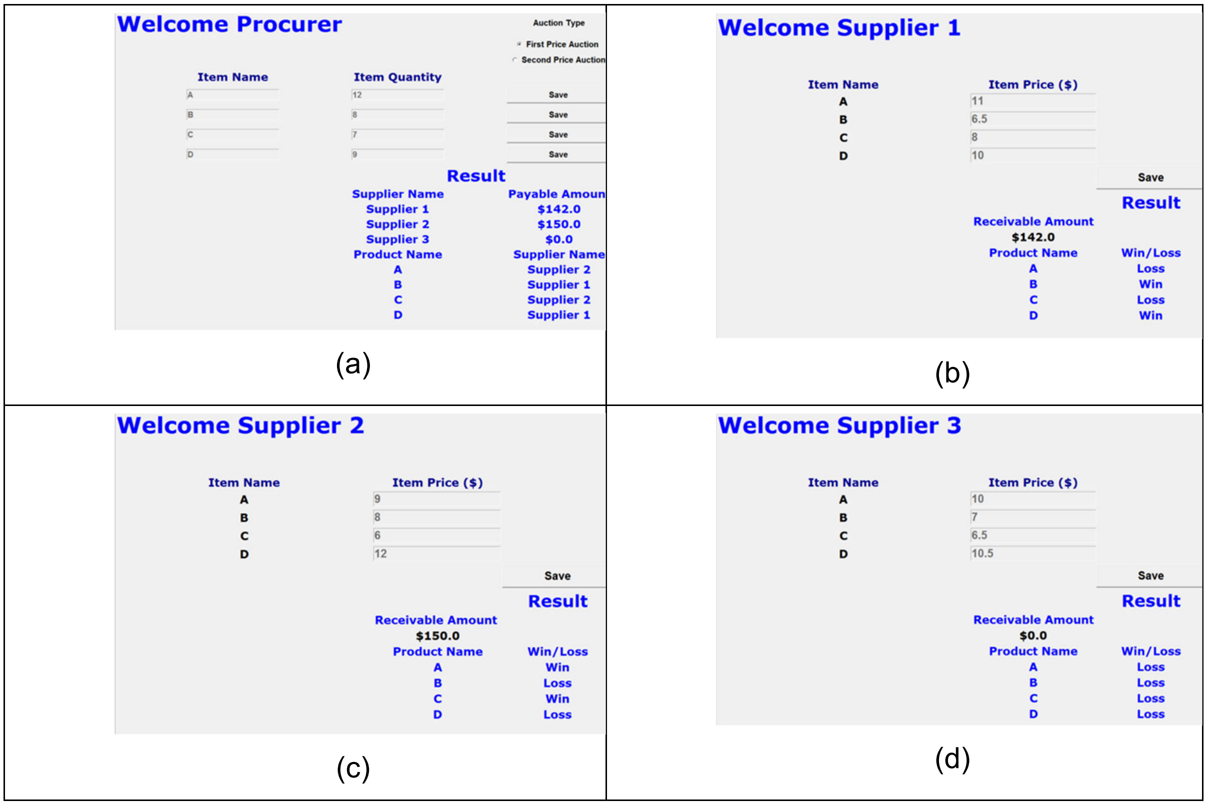


Figure 7. Demo of a CWR-First Price Reverse Auction

Deploying the CWR-first price reverse auction enables the procurer to enter item names and their respective quantities. Only the item names are provided to all the suppliers. Suppliers enter their respective confidential item prices (as listed in Table 4). As described in Protocol 1, the confidential information (item quantities and prices) is split additively and shared with the external servers (α and β). These external servers along with the help of another external server (γ) execute the computations involved in the auction. By the end of these computations, the procurer learns that items (A, C) and (B, D) will be provided by Supplier 2 and Supplier 1, respectively. The procurer also learns the amounts that should be paid to Supplier 1 and Supplier 2. The suppliers also receive information on the items they won/lost and their receivable payout amounts from the procurer. Figure 9 shows the screenshots of the procurer and suppliers at the end of the auction process. Note that throughout the procurement process, suppliers need not disclose their individual item prices to anyone.



Welcome Procurer

Auction Type
● First Price Auction
○ Second Price Auction

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

Result

Supplier Name	Payable Amoun
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

(a)

Welcome Supplier 1

Item Name	Item Price ($)
A	11
B	6.5
C	8
D	10

Save

Result

Receivable Amount
$142.0

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

(b)

Welcome Supplier 2

Item Name	Item Price ($)
A	9
B	8
C	6
D	12

Save

Result

Receivable Amount
$150.0

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

(c)

Welcome Supplier 3

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

(d)

Figure 8. Screenshots of the Procurer's Screen (a) and the Suppliers' Screens (b)–(d)

This CWR-first price reverse auction enables procurers to select the suppliers who provide the best price for each individual item. Such selection enables the procurer to reduce procurement costs. For instance, using the values listed in Table 4, CWR-first price reverse auction enables the procurer to procure all the desired items for $292 instead of $316 (from traditional sealed-bid auctions). We believe that this form of cherry-picking enables the procurer to increase competition among suppliers and thereby achieve efficient solutions.

We extended the functionality of this software embodiment to handle second-price reverse auctions by modifying the calculation of payments in Protocol 1. We tested the scalability of the proposed CWR-first price reverse auction by running for different numbers of items procured by the procurer. The resulting computational time and bandwidth use are reported in Tables 5 and 6, respectively. These results indicate that CWR-first price reverse auction is a computationally efficient and secure technique that can be deployed in real-time settings.

Table 5. Comparison of Bandwidth Use (KB)

Number of items	CWR: First Price	CWR: Second Price
4	7.8	7.2
8	8.2	8.7
16	9.2	9.5
32	15.3	12.58
64	18.95	18.41

Table 6. Comparison of Average Computational Time (in Seconds)

Number of items	CWR: First Price	CWR: Second Price
4	0.05	0.06
8	0.11	0.13
16	0.21	0.22
32	0.40	0.42
64	0.76	0.82

The CWR-first price reverse auction is a step towards demonstrating that computations in a procurement process can be performed without needing to reveal any confidential information. We believe that procurers and suppliers can build on this and modify it to make it suitable for more sophisticated computations.

Summary

The proposed approach, Computing-Without-Revealing (CWR), supports research in information systems and risk management. Our approach also complements, but does not replace, research in economic mechanism design. While mechanism design is focused on truthful revelation through the design of incentives, our approach focuses on protecting confidential information in any mechanism. In this study, we developed new dedicated CWR protocols suited for eProcurement and demonstrated the application of these protocols for the procurement of standard products. We believe that these protocols could be extended to the procurement of innovative technologies.

We present the CWR-first price reverse auction, which enables a procurer to “cherry pick” those suppliers who provide the best price for each individual item and thereby lower procurement costs. Such lowering of acquisition costs for procurers will increase their efficiency because they will be able to achieve more with the same financial resources.

Suppliers who participate will not see their competitive advantage erode due to the very fact that they participated (e.g., currently, a cost advantage for some components quickly erodes once it becomes known). The eProcurement platforms based on the proposed approach will considerably mitigate the threat of data breach originating from business partners because the approach makes it possible to achieve the desired collaborative goals with business partners without revealing to them the confidential data on which the collaboration depends.

A test bed is developed to compare the performance of CWR-based protocols with the previous-best approaches. Experimental results show that the CWR protocols performed better than previous-best approaches. With this, we conclude that CWR based auctions are lightweight, scalable, and secure.

Protocol 1: CWR-First Price Reverse Auction

Input: Procurer provides the list of items (denoted by **I**) and their respective quantities (denoted by $\mathbf{q} = [q_1, \ldots, q_N]$). Suppliers ($S_1, \ldots, S_K$) provide their item prices for the items in the list **I**. Supplier S_k item price list is denoted by $\mathbf{p_k} = [p_{k1} , \ldots, p_{kN}]$.

Output: Procurer determines the items won (represented by $\mathbf{w_k}$) by each supplier S_k and payment (represented by a_k).

Stage 1. Pre-processing of inputs

Step 1: The procurer and suppliers mutually identify cloud servers (α and β) as their surrogates to execute procurement using CWR. The procurer splits their sensitive information $\mathbf{q}$ into $\mathbf{q}_\alpha$ and $\mathbf{q}_\beta$ such that $\mathbf{q} = \mathbf{q}_\alpha + \mathbf{q}_\beta$ and shares them with the cloud servers α and β, respectively; [[.]] notation is used to represent these shares, [[**q**]] represents $\mathbf{q}_\alpha$ for cloud server α and $\mathbf{q}_\beta$ for cloud server β respectively. Similarly, the suppliers split their individual item price list and share them with the cloud servers α and β, respectively.

Step 2: Cloud servers (α and β) mutually agree upon morphing functions (M_α, M_β) and a seed to generate the random numbers that are used in these morphing functions. These agreements can be derived using session number, auction ID, etc. Further, the cloud servers (α and β) identify another cloud server (γ) as their helper to perform the desired procurement computations using CWR.

Stage 2. Run desired computations securely

Step 3: Cloud servers ($\alpha, \beta,$ and γ) execute the computations as mentioned in Table 7. Cloud servers (α and β) keep track of the splits corresponding to the information on whether a supplier S_k won/lost the items ($\mathbf{w_{\alpha k}} = [w_{\alpha 1}, \ldots, w_{\alpha N}]$**,** $\mathbf{w_{\beta k}}$) and the splits corresponding to the payments that are to be made to the supplier S_k ($a_{\alpha k}$, $a_{\beta k}$). The vector ($\mathbf{w_k} = \mathbf{w_{\alpha k}} + \mathbf{w_{\beta k}}$) has 1s against the items that are won and 0s against all the items lost by the supplier S_k.

Step 4: By the end of Step 3, cloud server α has ($\mathbf{a_\alpha} = [\, a_{\alpha 1}, \ldots, a_{\alpha k}]$, $\mathbf{W_\alpha} = [\, \mathbf{w_{\alpha 1}}, \ldots, \mathbf{w_{\alpha K}}]$) and cloud server β has ($\mathbf{a_\beta}$, $\mathbf{W_\beta}$)**.** Both cloud servers (α and β) share their splits with the procurer. The procurer adds ($\mathbf{a_\alpha}$**,** $\mathbf{a_\beta}$) to determine $\mathbf{a} = [a_1, \ldots, a_K]$ where a_k refers to the money that the procurer owes the supplier S_k. Similarly, the procurer adds **(**$\mathbf{W_\alpha}$, $\mathbf{W_\beta}$**)** to determine $\mathbf{W} = [\mathbf{w_1}, \ldots, \mathbf{w_K}]$.

Stage 3. Post-processing of outputs

Step 5: Procurers provide the payment a_K and items won (represented by $\mathbf{w_k}$) to S_k. Supplier S_k verifies the payment a_K against the item prices that he/she won.

Correctness

The correctness is derived from the correctness of CWR protocols.

Security

Procurer knows **q, a,** and **W**. With this information, the procurer cannot infer the suppliers' item prices. Similarly, suppliers receive $\mathbf{w}_{\mathbf{k}}$ and the items they need to provide to the procurer. Additionally, the suppliers cannot infer each other's private information such as item price. All the external servers ($\alpha, \beta,$ and γ) receive only one of the additive splits. However, these external servers learn the number of suppliers participating in the auction. This could be avoided by using different external servers for the computations.

Table 7. Psuedocode for Computations Performed on Cloud servers (α and β)

```
N→ number of items
K→ number of sellers
[[P]]→ NxK matrix with additive shares corresponding to prices from sellers for different items
[[Q]]→ additive shares corresponding to the quantity from Buyer
Winner_price = [0] * N # winning price for each item
W = [[0] * N] * K # winner index
item_paycheck = [0] * N
for j in range(N):
    [[index]]=0 # make Seller 1 as the default winner
    for i in range(1, K):
        [[b]]=0 # [[b]] denotes an additive share of b
        W [j][index], lowest_price = 1, [[P[j][index]]]
        [[b]]←CWR-GT0(lowest_price – [[P[j][i]]]) # update indices and prices
        W[j][i], W[j][index] = [[b]], [[1-b]]
        [[index]]=CWR-ADD(CWR-MP([[b]], [[i]]), CWR-MP([[1-b]], [[index]]))
        [[Winner_price[j]]] = CWR-ADD(CWR-MP([[b]], [[P[j][i]]]), CWR-MP([[1-b]], [[lowest_price]]))
    [[item_paycheck[j]]] = CWR-MP([[q[j]]], [[Winner_price[j]]])
a=[0]*K
for j in range(K):
    for i in range(N):
        [[b1]] = 0
        [[b1]]←CWR-EW0(j, W[i][j])
        [[a[j]]] = CWR-ADD([[a[j]]], CWR-MP([[item_paycheck[i]]], [[b1]]))
```

References

Ben-David, A., Nisan, N., & Pinkas, B. (2008, October). FairplayMP: A system for secure multi-party computation. In *Proceedings of the 15th ACM Conference on Computer and Communications Security* (pp. 257–266). Alexandria, VA: ACM.

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.

Bogetoft, P., Christensen, D. L., Damgård, I., Geisler, M., Jakobsen, T., Krøigaard, M., … Schwartzbach, M. (2009, February). Secure multiparty computation goes live. In *Proceedings of the International Conference on Financial Cryptography and Data Security* (pp. 325–343). Heidelberg, Germany: Springer.

Deshpande, V., Schwarz, L. B., Atallah, M. J., Blanton, M., & Frikken, K. B. (2010, October). Outsourcing manufacturing: Secure price-masking mechanisms for purchasing component parts. *Production and Operations Management, 20*(2), 165–180.

Kaestner, S., Arndt, C., & Dillon-Merrill, R. (2016, April). *The cybersecurity challenge in acquisition* (No. NPS-SYM-AM-16-041). Monterey, CA: Naval Postgraduate School.

Paillier, P. (1999, May). Public-key cryptosystems based on composite degree residuosity classes. In *Proceedings of the International Conference on the Theory and Applications of Cryptographic Techniques* (pp. 223–238). Heidelberg, Germany: Springer.

Ponemon Institute. (2016, August). *Closing security gaps to protect corporate data: A study of US and European organizations.* Retrieved from https://info.varonis.com/hubfs/docs/research_reports/Varonis_Ponemon_2016_Report.pdf

Wang, S., Bhandari, S., Chaduvula, S. C., Atallah, M. J., Panchal, J. H., & Ramani, K. (2017, June). Secure collaboration in engineering systems design. *Journal of Computing and Information Science in Engineering, 17*(4), 041010–041010-11.

Wang, S., Nassar, M., Atallah, M., & Malluhi, Q. (2013, November). Secure and private outsourcing of shape-based feature extraction. In *International Conference on Information and Communications Security* (pp. 90–99). Cham, Switzerland: Springer.

ACQUISITION RESEARCH PROGRAM
GRADUATE SCHOOL OF BUSINESS & PUBLIC POLICY
NAVAL POSTGRADUATE SCHOOL
555 DYER ROAD, INGERSOLL HALL
MONTEREY, CA 93943

www.acquisitionresearch.net