

Access to this work was provided by the University of Maryland, Baltimore County (UMBC) ScholarWorks@UMBC digital repository on the Maryland Shared Open Access (MD-SOAR) platform.

Please provide feedback

Please support the ScholarWorks@UMBC repository by emailing scholarworks-group@umbc.edu and telling us what having access to this work means to you and why it's important to you. Thank you.

A Secure Multi-Unit Sealed First-Price Auction Mechanism

Maya Larson¹, Wei Li¹, Chunqiang Hu¹, Ruinian Li¹, Xiuzhen Cheng¹, and
Rongfang Bie²

¹Department of Computer Science, The George Washington University,
Washington DC, USA

{maya_, weili, chu, ruinian, cheng}@gwu.edu

²College of Information Science and Technology, Beijing Normal University,
Beijing, China
rfbie@bnu.edu.cn

Abstract. Due to the popularity of auction mechanisms in real-world applications and the increase in the awareness of securing private information, auctions are in dire need of bid-privacy protection. In this paper, we deliberately design a secure multi-unit sealed-bid first-price auction scheme, in which the auction is processed on the bidders' encrypted bids by the server and the final output is only known by the auctioneer. As a result, neither the auctioneer nor the server can obtain the full information of the bidders. What's more, the auctioneer can verify whether a winner pays its full payment in the auction. Finally, a comprehensive analysis on the performance of our auction mechanism is conducted.

Keywords: secure auction, bid-privacy preserving, sealed-bid first-price auction, homomorphic encryption.

1 Introduction

In past decades, auction mechanisms have been a particularly successful application of game theory to the real world, with its uses ranging from eBay auctions on personal items, such as phones and laptops, to those which sell treasury bonds, rights to use radio spectrums, and schedule and allocate transportations.

Typically, an auction is centrally controlled by an auctioneer and bidders are supposed to faithfully reveal their valuations of the goods in the auction [9, 10, 15, 16]. However, the true valuations of goods are the private information of the bidders. Therefore, a secure auction must preserve the bid-privacy as once the valuations are revealed to an insincere auctioneer, it may exploit such knowledge for its own benefit either in future auctions or by reneging on the sale [17]. Sealed-bid auctions prevent releasing private information to other bidders, not the auctioneer, who keeps the information in hand even after the auction. With such information, the auctioneer can commit frauds by overcharging/underpaying the winning buyers/sellers with a forged price for its personal monetary gain.

Therefore, it is critical to design privacy-preserving auctions to protect the bid privacy and secure the auction. For this purpose, a number of secure auctions have been proposed [2, 8, 11, 13, 18, 20, 21, 23]. However, there are still some weaknesses in these approaches. For example, in [20], the auctioneer can decrypt all bidder's bids as the bids are encrypted with the auctioneer's public key; in [8], the auctioneer can know the bids of all buyer groups and their ranking order in the auction.

In this paper, we intend to design a secure multi-unit sealed-bid first-price auction with the consideration of homogeneous and heterogeneous goods. In our auction framework, a trust-worthy server is brought to compute the auction result for the auctioneer, so that the auctioneer only knows the final auction result without awareness of other bidders' bids. Since the server carries out computation on the encrypted bids, it learns nothing about the bidders' actual bids. Through this way, the bidders' bid can be preserved. Moreover, the auctioneer can verify whether a winner pays the full payment for its allocated goods.

The rest of this paper is organized as follows. Section 2 briefly summarizes related work. Section 3 introduces the preliminaries about the sealed-bid first-price auction and the homomorphic cryptosystem. Our auction model and auction scheme are presented in Sections 4 and 5, respectively. After analyzing the auction performance in Section 6, this paper is concluded in Section 7.

2 Related Work

In auction mechanisms, bid privacy is mainly protected via cryptographic tools, such as symmetric encryption, homomorphic encryption, and secret sharing [3, 22], etc.

By introducing a trust-worthy party in the auction, [2, 8] propose secure McAfee-based double auctions such that no party in the auction has the knowledge to obtain any sensitive information. Their major difference is that [8] employs the order preserving encryption and the oblivious transfer and [2] utilizes the Paillier cryptosystem. In [20, 21], the authors mask the bidding prices with a vector of ciphertext, and ensure that the auctioneer can find the maximum value, randomize the bids, and charge the bidders securely based on homomorphic encryption. However, in [20], the auctioneer can decrypt all bidder's bids, because the bids are encrypted with the auctioneer's public key; in [8], the auctioneer can know the bids of all buyer groups and their ranking order in the auctions.

In [11, 14, 23], the authors hide bidding prices with secret sharing, which is a useful cryptographic tool and is utilized in many applications such as body area network [5, 7], attribute-based encryption [6, 7], image security [4] and so on. However, there are two shortcomings in [11]: i) the scheme can not handle relationships among multiple winners; and ii) it is not computationally efficient. In [23], the authors hide the bids as the degree of polynomials. However, this scheme is limited to the passive adversary model, and the evaluators have to obtain their shares from a third party via a secure channel, so this scheme can not resist collusion attacks. Therefore, this scheme is not practical. In [18], the au-

thors apply verifiable secret sharing to construct sealed-bid auctions. The scheme provides verification to resist collusion attacks among the evaluators. Because the evaluators obtain their secret shares from a third party via a private secure channel, the scheme is vulnerable to collusion attacks between evaluators and the third party. We present a scheme to secure auctions without an auctioneer via verifiable secret sharing in our pervious work [13], which can resist passive attacks and collusion attacks and not require a secure channel.

3 Preliminaries

3.1 Sealed First-Price Auction

The sealed first-price auction is an efficient auction [1, 12]. In a multi-unit sealed auction, all bidders simultaneously submit their sealed bids to the auctioneer in advance of a deadline, without knowledge of any of their opponents' bids. After the deadline, the auctioneer unseals the bids and determines the clearing price at which demand equals supply. Each bidder wins the quantity demanded at the clearing price and pays the payment that he bids for the corresponding units of the goods.

This type of auction is used for refinancing credit and foreign exchange. The U.S. Treasury uses the sealed first-price auction to sell most of the treasury bills, notes, and bonds that finance the national debt of the United States.

3.2 Homomorphic Encryption

Homomorphic encryption is a form of encryption that enables the decrypted result computed on the ciphertext to match the result calculated on the plaintext. In addition, we require that such a homomorphic encryption is randomized and indistinguishable.

– Paillier Cryptosystem

In this paper, we adopt a Paillier cryptosystem [19], (G, E, D) , in which G is the key generation algorithm, E is the encryption algorithm, and D is the decryption algorithm. The Paillier cryptosystem works as follows [19]:

i) *Key Generation G*: Set $n = pq$ and $\lambda = \text{lcm}(p-1, q-1)$ where p and q are two large primes and lcm represents the least common multiple. Select a random number $g \in \mathbb{Z}_{n^2}^*$, such that $\text{gcd}(L(g^\lambda \bmod n^2), n) = 1$, in which $L(\cdot)$ is function defined as $L(k) = (k-1)/n$. The public and the private keys are (n, g) and (p, q) , respectively.

ii) *Encryption E*: Let m be the plaintext and $r \in \mathbb{Z}_n^*$ be a random number, the ciphertext c is

$$c = E(m, r) = g^m \cdot r^n \bmod n^2.$$

iii) *Decryption D*: For a ciphertext, the corresponding plaintext can be decrypted as

$$m = D(c) = \frac{L(c^\lambda \bmod n^2)}{L(g^\lambda \bmod n^2)} \bmod n.$$

The Paillier encryption has randomizability, indistinguishability, and the following *homomorphic properties*:

$$D(E(m_1, r_1)E(m_2, r_2) \bmod n^2) = m_1 + m_2 \bmod n,$$

where m_1 and m_2 are two plaintexts, and r_1 and r_2 are two random numbers.

– **Encrypted Vector**

For a vector $x_i = (x_{i1}, x_{i2}, \dots, x_{ik})$, its ciphertext is represented as follows:

$$\mathbf{e}(x_i) = (e_{i1}, e_{i2}, \dots, e_{im}) = (E(x_{i1}), E(x_{i2}), \dots, E(x_{ik})).$$

Since E is indistinguishable, we cannot identify the value of x_i without decrypting each element. Accordingly, the component-wise product of $\mathbf{e}(x_1)$ and $\mathbf{e}(x_2)$ is

$$\mathbf{e}(x_1)\mathbf{e}(x_2) = (e_{11}e_{21}, e_{12}e_{22}, \dots, e_{1k}e_{2k}).$$

For a general case, we have

$$\begin{aligned} \prod_i \mathbf{e}(x_i) &= (\prod_i \mathbf{e}(x_{i1}), \prod_i \mathbf{e}(x_{i2}), \dots, \prod_i \mathbf{e}(x_{ik})) \\ &= (\prod_i E(x_{i1}), \prod_i E(x_{i2}), \dots, \prod_i E(x_{ik})). \end{aligned} \quad (1)$$

4 Auction Model

We consider a market with a set of homogeneous goods denoted by \mathcal{Q} ($|\mathcal{Q}| = Q$), in which a set of bidders denoted by \mathcal{M} ($|\mathcal{M}| = M$) bid for the goods, an auctioneer takes charge of the auction process, and a server performs computation in the auction. From the original sealed first-price auction, we can see that the auctioneer can know all bidders' information, which is a risk to bidder's privacy. Thus, to prevent information leakage in the auction, we employ the server to calculate the auction result for the auctioneer.

The homogeneity of all goods means that each individual good is identical and that all goods have the exactly same characteristics. Consequently, bids can be expressed in terms of prices that the bidder is willing to pay for some units of the homogeneous goods, without indicating the identity of the particular good that is desired. Formally, let $\mathcal{M}^Q = \{A : \mathcal{Q} \rightarrow \mathcal{M}\}$ be the set of allocations of goods \mathcal{Q} to bidders \mathcal{M} .

Suppose that bidder i 's evaluation function is $f_i : \mathcal{M}^Q \rightarrow \mathbb{Z}^+$; that is, for each assignment $A \in \mathcal{M}^Q$, bidder i 's bid value is $b_i(A)$. For any bidder i , f_i is private and is not revealed to others. In addition, any bidder i 's evaluation function is independent to others, implying that bidder i decides the function f_i by itself without the impact from others.

Different from some previous work that considers the third party is trustworthy, the auctioneer and the server in our model may be adversaries who intend to steal bidders' private information. Therefore, our main idea to preserve privacy is that the auctioneer only knows the winners and their payments, and that the server only processes the calculation without leaning bidders' information.

5 Secure Auction Mechanism

In this section, we propose a secure multi-unit sealed first-price auction mechanism, in which there are five major stages including *initiation*, *bidding*, *computation*, *winner determination*, and *payoff*. An overview of our auction mechanism is presented in Fig. 1.

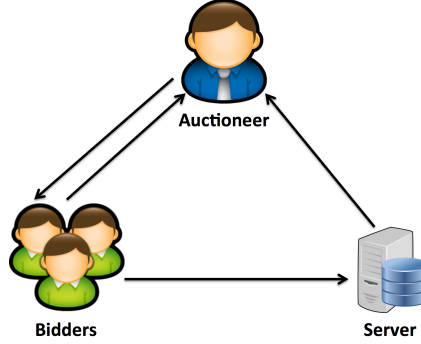


Fig. 1. An overview of the proposed auction mechanism.

As shown in Fig. 1, all necessary information is prepared at the initiation stage. Then, the server receives the encrypted bids from all bidders, computes the auction results, and sends the encrypted results to the auctioneer. Based on the results, the auctioneer determines the winners and assignments. Finally, all winners pay the payments to the auctioneer. Note that in this paper, we assume that there is no collusion activity among the bidders, the auctioneer, and the server in the auction.

5.1 Initiation

The auctioneer generates its secret and public keys of homomorphic encryption E via G , and publishes the corresponding public key based on E and the set of possible assignments \mathcal{M}^Q .

At the same time, the server also generates its secret key K_s based on RSA public-key cryptosystem, and public key K_p , and announces K_p .

5.2 Bidding

Each bidder i encrypts the bid value $b_i = (b_i(A_1), b_i(A_2), \dots, b_i(A_{|\mathcal{M}^Q|}))$ by using Paillier encryption E first and then the server's public key K_p , outputs $K_p(\mathbf{e}(b_i))$, and sends $K_p(\mathbf{e}(b_i))$ to the server directly. Since each bid value vector b_i is encrypted twice and there is no collusion between the auctioneer and the server, neither the auctioneer nor the server can learn the actual value of b_i .

5.3 Computation

After receiving the encrypted bid values from all bidders, the server decrypts $K_p(\mathbf{e}(b_i))$ for $1 \leq i \leq M$ with its secret key K_s , gets $\mathbf{e}(b_i)$, and calculates the sum of bid values for each assignment in \mathcal{M}^Q as follows:

$$\begin{aligned} \prod_i \mathbf{e}(b_i) &= (\prod_i \mathbf{e}(b_i(A_1)), \prod_i \mathbf{e}(b_i(A_2)), \dots, \prod_i \mathbf{e}(b_i(A_{|\mathcal{M}^Q|}))) \\ &= (\prod_i E(b_i(A_1)), \prod_i E(b_i(A_2)), \dots, \prod_i E(b_i(A_{|\mathcal{M}^Q|}))). \end{aligned} \quad (2)$$

As the server cannot decrypt the homomorphic encryption, it cannot know any information of the result. Then, the server sends the result of $\prod_i \mathbf{e}(b_i)$ to the auctioneer.

5.4 Winner Determination

The auctioneer performs the decryption on $\prod_i \mathbf{e}(b_i)$ and obtains:

$$\begin{aligned} D(\prod_i \mathbf{e}(b_i) \mod n^2) &= (D(\prod_i \mathbf{e}(b_i(A_1)) \mod n^2), \dots, D(\prod_i \mathbf{e}(b_i(A_{|\mathcal{M}^Q|})) \mod n^2)) \\ &= (\sum_i b_i(A_1) \mod n, \dots, \sum_i b_i(A_{|\mathcal{M}^Q|}) \mod n) \\ &= (\sum_i b_i(A_1), \dots, \sum_i b_i(A_{|\mathcal{M}^Q|})). \end{aligned} \quad (3)$$

According to the decrypted result, the auctioneer selects the maximum value, Sum^* , and the corresponding assignment A^* , i.e.,

$$\begin{aligned} Sum^* &= \max\{\sum_i b_i(A_1), \sum_i b_i(A_2), \dots, \sum_i b_i(A_{|\mathcal{M}^Q|})\}, \\ A^* &= \arg \max\{\sum_i b_i(A_1), \sum_i b_i(A_2), \dots, \sum_i b_i(A_{|\mathcal{M}^Q|})\}. \end{aligned}$$

That is, Sum^* is the maximum sum of bidders' evaluation values, and goods are sold according to A^* in the auction. Furthermore, based on the allocation A^* , the auctioneer can determine the set of winners, \mathcal{W} .

5.5 Payoff

The auctioneer announces the winners and the allocation, and collects the payments from all winners. If bidder i is a winner, it pays a price of $b_i(A^*)$ to the auctioneer; otherwise, it pays nothing.

Since the auctioneer only knows the value of Sum^* rather than $b_i(A^*)$ for all winning bidders, the auctioneer cannot judge whether each winner pays a

full payment or not. Denote by p_i the payment of bidder i in the auction. If $Sum^* \neq \sum_{i \in W} p_i$, the auctioneer can utilize the following “*payment checking*” process to check whether p_i is equal to $b_i(A^*)$ or not: the auctioneer sends a request to the server, to get $e(b_i(A^*)) = E(b_i(A^*))$ for all $i \in W$; the server returns all required information to the auctioneer; then, the auctioneer decrypts $E(b_i(A^*))$ and obtains $b_i(A^*)$; and the auctioneer can find out which winner does not pay the full price via a comparison.

Example

Finally, we use a toy example to demonstrate our auction mechanism. Suppose $Q = 2$, $\mathcal{M} = \{1, 2\}$, and $\mathcal{M}^Q = \{(0, 2), (1, 1), (2, 0)\}$. Two bidders’ bids are $b_1 = (0, 3, 5)$ and $b_2 = (4, 3, 0)$, respectively. At the beginning of the auction, these two bidders submit $K_p(\mathbf{e}(b_1))$ and $K_p(\mathbf{e}(b_2))$ to the server. The server decrypts the bids, carries out a computation on the ciphertexts $\mathbf{e}(b_1)$ and $\mathbf{e}(b_2)$, and gets the following result:

$$\mathbf{e}(b_1)\mathbf{e}(b_2) = (e(0)e(4), e(3)e(3), e(5)e(0)).$$

Next, the server returns the result to the auctioneer. The auctioneer decrypts the result and gets a vector of $(4, 6, 5)$. Accordingly, the maximum value is $Sum^* = 6$ and the corresponding assignment is $A^* = A_2$; that is, bidders 1 and 2 can respectively win one unit of the goods. Finally, bidder 1 pays 3 and bidder 2 pays 3 to the auctioneer.

5.6 Extension to Heterogeneous Markets

Our proposed secure multi-unit sealed first-price auction can be easily extended to a heterogeneous market, in which goods have different characteristics. Thus, the assignment considers not only how many units of the goods, but also which units of goods, leading to a larger set of possible assignments \mathcal{M}^Q . Except for this, the auction process is the same as that of the proposed secure multi-unit homogeneous sealed first-price auction.

6 Performance Analysis

6.1 Security

In this subsection, we investigate the security issues of our proposed auction mechanism from the following aspects.

Due to the randomizability and the indistinguishability of the encryption E in the Paillier cryptosystem, the same message can be encrypted into different ciphertexts by using different random blinding factors r , indicating that such an encryption scheme can resist dictionary attacks. In addition, since each bidder’s bid is a vector and we separately encrypt every element of the bid vector, any bidder’s bid vector can be kept secret unless every encrypted element of the bid vector is revealed.

Neither the auctioneer nor the server can learn the full information of bidders. On one hand, the auctioneer knows the final winners and their bids for the allocated goods (not the bid vectors of winners); on the other hand, the server computes the auction result based on the encrypted bids not the plaintexts. As a result, in the collusion-free market, our proposed auction scheme can secure the information of bidders.

The auctioneer can verify the bids of winners with the help of the server. According to the pricing method of the sealed-bid first-price auction, each winner's payment is the bid value for the allocated goods. When the amount of payments collected from the winners does not equal the calculated auction result, the auctioneer can decrypt the encrypted bids that are requested from the server and check whether each winner pays the full price or not. Therefore, the winners cannot cheat on payments in the auction.

6.2 Efficiency

The communication and the computational complexities of our auction mechanism are analyzed as follows.

- **Communication Complexity**

At the bidding stage, all bidders report their encrypted bids to the server at the same time and the communication volume of each bidder is $O(|\mathcal{M}^Q|)$, thus the communication volume of this stage is $O(|\mathcal{M}| \cdot |\mathcal{M}^Q|)$, where $|\mathcal{M}|$ is the number of bidders, Q is the number of goods, and $|\mathcal{M}^Q|$ is the number of possible assignments in the auction. At the computation stage, the communication volume between the server and the auctioneer is $O(|\mathcal{M}^Q|)$. Since all winners simultaneously submit their payments to the auctioneer at the payoff stage, the communication volume $O(|\mathcal{W}|)$, in which $|\mathcal{W}|$ is the number of winners. If the auctioneer needs to perform the payment checking process, the corresponding communication volume is $O(1)$.

- **Computational Complexity**

For each bidder, it needs to calculate $|\mathcal{M}^Q|$ bids in the auction, leading to a computational complexity of $O(|\mathcal{M}^Q|)$. For the server, it computes the sum of all bidders' encrypted bids within $O(|\mathcal{M}| \cdot |\mathcal{M}^Q|)$. For the auctioneer, the computational complexity of searching for the maximum value is $O(|\mathcal{M}^Q|)$ and the computational complexity of the payment checking process is $O(|\mathcal{W}|)$.

7 Conclusion

In this paper, we propose a secure multi-unit sealed-bid first-price auction. By employing a server that computes the auction result based on the encrypted bids, our secure auction mechanism can protect the private bids from both the server and the auctioneer. In addition, our auction supports the verification of winners' payments for the auctioneer; that is, the auctioneer can check whether a winner

pays its full price for its allocated goods. Finally, we evaluate the performance of our proposed auction scheme in terms of security, communication complexity, and computational complexity.

In our work, the scheme does not consider collusion activity among the bidders, the auctioneer, and the server. In future work, we will consider how to defense collusion attacks when there is collusion activity in the auction.

Acknowledgment

The authors would like to thank all the reviewers for their helpful comments. This project was supported by the US National Science Foundation (ECCS-1407986, AST-1443858, CNS-1265311, and CNS-1162057), and the National Natural Science Foundation of China (61171014).

References

- [1] Ausubel, L.M.: New Economy Handbook, chap. 6: Auction Theory for the New Economy. Academic Press (2003)
- [2] Chen, Z., Huang, L., Li, L., Yang, W., Miao, H., Tian, M., Wang, F.: Ps-trust: Provably secure solution for truthful double spectrum auctions. In: IEEE INFOCOM. pp. 1249–1257 (2014)
- [3] Hu, C., Liao, X., Cheng, X.: Verifiable multi-secret sharing based on LFSR sequences. Theoretical Computer Science 445, 52–62 (2012)
- [4] Hu, C., Liao, X., Xiao, D.: Secret image sharing based on chaotic map and chinese remainder theorem. International Journal of Wavelets, Multiresolution and Information Processing 10(03), 1250023(1–18) (May 2012)
- [5] Hu, C., Zhang, F., Cheng, X., Liao, X., Chen, D.: Securing communications between external users and wireless body area networks. In: Proceedings of the 2nd ACM workshop on Hot topics on wireless network security and privacy. pp. 31–36. ACM (2013)
- [6] Hu, C., Zhang, F., Xiang, T., Li, H., Xiao, X., Huang, G.: A practically optimized implementation of attribute based cryptosystems. In: 2014 IEEE 13th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom). pp. 197–204. IEEE (2014)
- [7] Hu, C., Zhang, N., Li, H., Cheng, X., Liao, X.: Body area network security: A fuzzy attribute-based signcryption scheme. Selected Areas in Communications, IEEE Journal on 31(9), 37–46 (2013)
- [8] Huang, Q., Tao, Y., Wu, F.: Spring: A strategy-proof and privacy preserving spectrum auction mechanism. In: IEEE INFOCOM. pp. 851–859. Turin, Italy (April 2013)
- [9] Jing, T., Zhang, F., Ma, L., Li, W., Chen, X., Huo, Y.: Tora: Truthful online reverse auction with flexible preemption for access permission transaction in macro-femtocell networks. In: WASA. pp. 512–523. Zhangjiajie, China (August 2013)
- [10] Jing, T., Zhao, C., Xing, X., Huo, Y., Li, W., Cheng, X.: A multi-unit truthful double auction framework for secondary market. In: IEEE ICC (2013)
- [11] Kikuchi, H.: $(m+1)$ -st-price auction protocol. Financial Cryptography 2339, 351–363 (2002)

- [12] Krishna, V.: Auction Theory. Elsevier, 2 edn. (2010)
- [13] Larson, M., Hu, C., Li, R., Li, W., Cheng, X.: Secure auctions without an auctioneer via verifiable secret sharing. In: Workshop on Privacy-Aware Mobile Computing (PAMCO) 2015 In conjunction with ACM MobiHoc 2015. ACM (2015)
- [14] Larson, M., Li, R., Hu, C., Li, W., Cheng, X.: A bidder-oriented privacy-preserving vcg auction scheme. In: The 10th International Conference on Wireless Algorithms, Systems, and Applications (WASA 2015). Springer (August 2015)
- [15] Li, W., Cheng, X., Bie, R., Zhao, F.: An extensible and flexible truthful auction framework for heterogeneous spectrum markets. In: ACM MobiHoc. pp. 175–184. Philadelphia, USA (August 2014)
- [16] Li, W., Wang, S., Cheng, X., Bie, R.: Truthful multi-attribute auction with discriminatory pricing in cognitive radio networks. ACM SIGMOBILE Mobile Computing and Communications Review 18(1), 3–13 (January 2014)
- [17] Naor, M., Pinkas, B., Sumner, R.: Privacy preserving auctions and mechanism design. In: the 1st ACM conference on Electronic commerce. pp. 129–139 (1999)
- [18] Nojoumian, M., Stinson, D.R.: Efficient sealed-bid auction protocols using verifiable secret sharing. Information Security and Experience 8434, 302–317 (2014)
- [19] Paillier, P.: Public-key cryptosystems based on composite degree residuosity classes. In: EUROCRYPT. vol. LNCS 1592, pp. 223–238 (1999)
- [20] Pan, M., Sun, J., Fang, Y.: Purging the back-room dealing: Secure spectrum auction leveraging paillier cryptosystem. IEEE Journal on Selected Areas in Communications 29(4), 866–876 (April 2011)
- [21] Pan, M., Zhu, X., Fang, Y.: Using homomorphic encryption to secure the combinatorial spectrum auction without the trustworthy auctioneer. Wireless Networks 18(2), 113–128 (2012)
- [22] Shamir, A.: How to share a secret. Communications of the ACM 22(11), 612–613 (1979)
- [23] Suzuki, K., Yokoo, M.: Secure combinatorial auctions by dynamic programming with polynomial secret sharing. Financial Cryptography 2357, 44–56 (2003)