Efficient Implementation and Computational Analysis of Privacy-Preserving Auction Protocols

Ramiro Alvarez and Mehrdad Nojoumian

Department of Computer & Electrical Engineering and Computer Science
Florida Atlantic University, Boca Raton, FL 33431, USA
{ramiroalvare2015,mnojoumian}@fau.edu

Abstract. Auctions are a key economic mechanism for establishing the value of goods that have an uncertain price. Nowadays, as a consequence of the ubiquitous emergence of technology, auctions can reach consumers, and as a result, drive market prices on a global scale. Collection of private information such as losing bids exposes more information than desired. In fact, the leaked information can be analyzed to provide auctioneers or competitors with advantages on future transactions. Therefore, the need to preserve privacy has become a critical concern to reach an accepted level of fairness and to provide market participants with an environment in which they can bid true valuations. This paper focuses on constructions of sealed-bid auctions based on cryptographic protocols. Instead of solely focusing on theoretical aspects of sealed-bid auctions, this paper dives into implementation details and demonstrates communication and computational analyses and how different settings affect performance.

Keywords: Sealed-bid auctions, privacy-preserving protocols, complexity.

1 Introduction

For many years auctions have existed as mechanism to trade commodities. At a minimum, an auction involves two groups: bidders and auctioneers. Auctioneers arrange the auctions, set the rules, and declare a winner after the price evaluation. Bidders are parties with an interest to acquire a certain good, or in the case of contractors, provide a service. The literature provides different classification for auctions, some of which are concisely described below.

The most common type of auction is the classical *English auction* involving an act where the bidders speculate and overestimate the price of an item in an open fashion. Usually seen in the sale of antiques and significant artwork, the auction start off at the reserve price and increases in an ascending manner when a bidder bids at that price. It proceeds increasing until no one is willing to pay a greater amount. The winner is the bidder willing to pay the highest price. In contrast, an auction with a price adjustment in a decreasing direction is labeled as *Dutch-style*. Most commonly, decreasing price auctions are observed in perishable markets such as fish and flowers where the interest is to sell an item before it expires. To begin, the auctioneer asks a high price for the item. The price is decreased if no one chooses to buy. The price continues to decrease in intervals until someone is willing to pay. The first willing volunteer will be the winner. Therefore, Dutch-style auctions inherently protect the loosing bids. Last but not least, sealed-bid auctions are the primary focus of this paper. The game changing rule is that bidders have one single opportunity to decide on a bid. This enforces a bidder to drop possible speculation and also reduces the bidding strategy to a true valuation. When the winner pays the standing price, this is referred to as the first-price. On the other hand a *Vickrey auction* states that the winner, being the highest bidder, pays the second highest price.

1.1 Our Motivation and Contribution

As stated in the literature, the main motivation for *sealed-bid actions* is to protect the losing bids as they can be used by auctioneers to maximize their revenues in future auctions. Although many works in the literature discuss theoretical approaches to sealed-bid auctions, the research on implementation is limited. Herein, our aim is to elucidate the intricate details of implementation and provide computational and communication analyses of several protocols. The protocols that were considered are [11, 23, 24]. For [11], two version were implemented with and without verification. For [23], there are also two implementations based on ElGammal and RSA. Finally, we conclude with an implementation of [24].
Rational for our selection: The main reason for our selection is because the first-price auction is still the most usable auction type that is widely used in settings such as e-commerce and ad auctions. Besides, the selected auctions utilize the most popular and strongest cryptographic primitives such as secure multiparty computation (MPC), public-key encryption, and undeniable signature schemes. The newer papers in the literature mainly focus on specific types of auctions, e.g., clock-proxy auctions and multi-unit auctions, or costly cryptographic primitives. These are two main reasons that we selected these protocols.
Our main contributions: An efficient implementation of the selected protocols is our primary contribution. We utilized the latest efficient implementations of cryptographic primitives such as SHA1, RSA and ElGamal, primitive root generator, safe prime generator, etc. Moreover, we separated the initialization time from the verification time to have a realistic comparisons among these protocols. Usually, initialization can be done offline without any limitation and that is why it should be evaluated separately. Finally, the way that we compared these protocols, i.e., price range parameters 25%, 50%, 75% and 100%, is our unique evaluation methodology that truly reveals the cons and pros of the selected protocols. In other words, an in-depth assessment of each auction is generated by modifying parameters such the modulus size, the number of bidders, and the price range. The results show that the complexity increases with modulus sizes as expected for all sealed-bid auctions. Interestingly, for [11], the complexity increases more with increases in the price ranges. We also observed that [24] has the highest communication complexity, as discussed later.

2 Brief Literature Review

Due to lack of space, we briefly review the literature. However, a comprehensive survey on privacy-preserving protocols for sealed-bid auctions is provided in [2].

Franking and Reiter introduced one of the early designs for sealed-bid auctions in [8]. The protocol relies on verifiable signature sharing [7] used to prevent bidders from denying their bids. Kikuchi et. al. created a first-price sealed-bid auction [12] based on the addition gate of secure MPC. Later, the protocol was modified by [13] to improve privacy, and by [21] to increase anonymity, fairness, and robustness. Nojoumian and Stinson [19] constructed efficient sealed-bid auction protocols based on addition and multiplication operations of verifiable secret sharing (VSS). The proposed solution works for a wide range of sealed-bid auctions. The authors of [6] use a homomorphic public-key encryption scheme. However, this protocol only works with pairwise comparison. With a similar approach, [23] utilizes a public-key cryptosystem to protect the losing bids. Another line of research focuses on sealed-bid Dutch-style auctions such as [18] that utilizes a multicomponent commitment scheme (MCS). The authors of [14] implemented and analyzed different Dutch-style sealed-bid auction protocols in both computationally and unconditionally secure models.

Under the category of Vickrey auctions, [16] proposes a protocol that relies on an oblivious third party. In this construction, the bidders must communicate between two servers. Bids are encrypted and the decryption keys are shared among auctioneers using secure MPC. The efficiency is improved by [15] substituting MPC with a homomorphic scheme. The problem of one of the two servers cheating is addressed in [10] by splitting the bid so that each server doesn't hold the entire information. Another set of protocols is designed to implement *$(M + 1)$-price auctions*. This is a type of auction in which M highest bidders take the prize and it is equivalent to the Vickrey auction when $M = 1$. Research works such as [11, 1, 5, 28] contain details on designing $(M + 1)$-proice auctions. The approach in [11] is to hide the bidding price in the degree of polynomials. The polynomials are shared and the the summation operation is used to construct a polynomial that holds the highest price in the degree. Another auction type, know as *combinatorial auction*, allows the bidders to place evaluations on a bundle of items. Combinatorial auctions can be multi-unit, linear good and general. For references on these auctions, we refer the readers to [9, 22, 25, 26].

3 Sealed-bid Auctions' Properties

As stated earlier, sealed-bid auctions describe a mechanism in which the bidders are given a chance to decide their final bidding values. Due to the nature of the mechanism, the bidders cannot gain knowledge from other bidders, thus they cannot create a strategy other than to bid a true valuation. Furthermore, the invention of the Internet connects users across nations and removes geological and space constrains, which exist in physical auctions. At the very least, an electronic sealed-bid auction must ensure concealment of losing bids, non-repudiation, verifiability, correctness and fairness, as illustrated in [17].

- **Privacy of Losing Bids**: Determination of the winner should not arrive at the expense of opening or decrypting the losing bids. In fact, a proper protocol should not reveal losing bids at all since this provides information to sellers, which can turn the tables in their favor in subsequent auctions.
- **Non-repudiation**: A bidder should not be able to deny sending a bid which was truly submitted.
- **Verifiability**: The winning bid should be recognized by all the bidders in the auction as being the true winning bid, and every bidder should have a method of verifying that others have followed the auction protocol accordingly.
- **Correctness**: The protocol should not determine an incorrect winner or winning price under any circumstances.
- **Fairness**: A subset of players should not have any advantage over others due to the manner that the protocol is constructed. Also the auctioneer should not have any advantage.

It is worth mentioning that if the security of the underlying cryptographic primitives rely on hardness of well-known mathematical problems such as integer factoring or discrete logarithm, the protocol will be *computationally secure*. However, if we don't have this condition, the protocol will be *unconditionally secure*.

4 Protocol Description

Next, we explain in detail the selected protocols that are the subject of our study.

4.1 Hiroaki Kikuchi's Protocol

The proposed construction, as shown in Figure 1, is based on the addition operation of secure MPC [3]. The protocol relies on a simple fact that if f and h are polynomials of degree t and s respectively, then $f + h$ has degree $max(t, s)$. First, a prime number p of order q is chosen. Auctioneers publish a price list W. Each bidder chooses a random polynomial from a finite field and the bidding value is equal to the degree of the polynomial. Each auctioneer receives a share from a bidder using secret sharing and computes a total sum, denoted as F over the shares. Because polynomials were chosen so that F's constant term was equal to zero, any party can find the smallest subset that produces a polynomial containing the highest bid as the degree of the polynomial.

The second version of the protocol, as explained in Figure 2, is made stronger with verifiable secret sharing of [20]. First, a prime p of order q is chosen same way as before, but now also two distinct primitive roots g_1 and g_2 are chosen and made publicly available. Bidder b_i chooses two randomly generated polynomials f and h. Each bidder makes a commitment of the polynomial by sending the multiplication of the powers of the primitive roots with the coefficients of the polynomials. For example, for polynomial $f(x) = a_1x + a_2x^2 + ... + a_t^t$ and $h(x) = b_1x + b_2x^2 + ... + b_s^s$, the bidders send $g_1^a g_2^b 1$, $g_1^a g_2^b 2$, until a commitment is made on all the coefficients. The sums F and H are calculated for the shares

Initialization

1. Establish field Z_p^* by choosing primes p and q such that q divides $p-1$, and operations are done using modular p.
2. The i^{th} bidder chooses $b_i \in \{1, ..., k\}$ and it is concealed by a random polynomial with degree $t_i = b_i + c$ and $a_0 = 0$, where c is the number of faulty auctioneers.

$$f_i(x) = \sum_{j=1}^{t_i} a_j x^j$$

Bid Submission

1. Each bidder evaluates and sends $f_i(\alpha_j)$ to auctioneers A_j for $j = 1, ..., m$.
2. Each auctioneer adds the shares received from the bidders and publishes $F(\alpha_j)$ by a commitment scheme.

$$F(\alpha_j) = \sum_{j=1}^{n} f_i(\alpha_j)$$

Winner Determination

1. Using the public values $F(\alpha_1), ..., F(\alpha_n)$, any entity can use Lagrange interpolation and construct a polynomial of degree $max(t_1, ..., t_n)$.
2. By subtracting parameter c, the highest bid is recovered.

Fig. 1. Hiroaki Kikuchi's Protocol.

received from f and h respectively. Auctioneers calculate $Y = g_1^F$ and $Z = g_2^H$ and publish YZ. The Lagrange Interpolation once again generates a polynomial that contains the highest bid in the degree. The main difference is that, with the extra computation to incorporate the verification protocol, neither auctioneers, nor bidders are permitted to insert fake values. Committing at every step of communication makes cheating detectable.

4.2 Kazue Sako's Protocol

Two practical cryptosystems, ElGamal and RSA, are used in the computationally secured sealed-bid auction of [23], shown in Figure 3. For each price in the price list, there is an associated public-key. For example, for price list $V = \{v_1, v_2, ..., v_L\}$, there are public-keys $PubK = \{pubk_1, pubk_2, ..., pubk_l\}$, and the auctioneers hold private keys $Pk = \{pk_1, pk_2, ..., pk_l\}$. In order to bid, a bidder uses the key associated with a price and encrypts the bid with that key. During the winner determination phase, the auctioneers pick the private-key associated with the highest price on the list and try to decrypt every submitted bid. A successful decryption determines the winner. If no winner is found at a specific price, the auctioneers pick the next highest private-key and reiterate the process. In order to make the protocol stronger, the authors suggest using the Shamir's secret sharing scheme [27] to split the keys into n shares and then give a share to each auctioneer to provide a mechanism of resilience against dishonest auctioneers who may decrypt bids.

Initialization

1. Establish field Z_p^*, primes p and generators g_1 and g_2.
2. The i^{th} bidder chooses bid $b_i \in \{1, ..., k\}$ and must commit on two polynomials. The polynomials are $f_i(x)$ of degree $t_i = b_i + c$ and $h_i(x)$ of degree $s = k + c$.

$$f_i(x) = \sum_{j=1}^{t_i} a_j x^j \;\; and \;\; h_i(x) = \sum_{j=1}^{s} b_j x^j$$

Bid Submission

1. Each bidder sends shares $f_i(\alpha_j)$ and $h_i(\alpha_j)$ to each participating auctioneer A_j for $j = 1, ..., m$.
2. Each bidder publishes public values that serve as commitments of his own polynomial.

$$E_{i,j} = g_1^{a_1 b_1}, ..., E_{i,t_i}$$

$$E_{i,t_i+1} = g_2^{b_{t_i+1}}, ..., E_{i,s}$$

Verification Step

1. Auctioneer j can verify that the share of bidder i is correct by verifying the polynomial commitment according to the following equation.

$$g_1^{f_i(\alpha_j)} g_2^{h_i(\alpha_j)} = \prod_{l=1}^{s} (E_{i,j})^{\alpha_j^t}$$

2. If verification holds, the auctioneers can proceed to compute and publish the sum of shares on $f(x)$ and $h(x)$.

$$F(\alpha_j) = \sum_{j=1}^{n} f_i(\alpha_j) \;\; and \;\; H(\alpha_j) = \sum_{j=1}^{n} h_i(\alpha_j)$$

3. The computed sum of shares can be verified by any entity using the following equality:

$$Y_j Z_j = g_1^{F(\alpha_j)} g_2^{H(\alpha_j)}$$

Winner Determination

1. The highest bid is the first element in the price list $\{1, ..., k\}$ that satisfies the equality below.

$$g_1^{F^{(t*)}(0)} = 1$$

where $F^{(t*)}(0)$ is obtained using Lagrange Interpolation

$$F^{(s)}(0) = \sum_{j=1}^{s} \prod_{i \neq j \in A_s} \frac{\alpha_i}{\alpha_i - \alpha_j} \qquad (1)$$

Fig. 2. Verifiable Version of Hiroaki Kikuchi's Protocol.

Initialization

1. Establish a price list and generate private and public-key pairs.
2. Publish the set of public-keys and arrange it such that each key matches a price in the price list.

Bid Submission

1. Each bidder chooses a public-key according to the price he intends to bid on.
2. The bidder encrypts the price with the key that is associated to that price according to the established mapping.

Winner Determination

1. Starting with the private-key that is associated with the highest price, the auctioneers decrypt each encryption that they have received. The elements decrypted to the value of the price in the current round are the highest bids.

Fig. 3. Kazue Sako's Protocol.

4.3 Sakurai's and Miyazaki's Protocol

The authors in [24] describe an auction, Figure 4, that can be built using a convertible undeniable signature scheme [4]. First, the protocol requires a safe prime p, a subgroup generator α and a one-way hash function. The prime p and the primitive root α are used to create secrets that are computationally secure based on the discrete logarithmic problem. The auction proceeds in a Dutch-style fashion. The verifier (auctioneer) and the prover (bidder) engage in several rounds of communications to prove equality or inequality against the standing price. Determination of equality or inequality does not reveal any private information since the auctioneer concludes based on the comparison of two discrete logs. At the time of winner determination, the bidders reveal their private keys, which further confirms correctness of the protocol.

5 Implementation Results

Our simulation was developed under JetBrains CLion environment. Our implementations were written in C++ and compiled under GNU GCC compiler. For an efficient implementation, we utilized the Crypto++ library. For instance, we made extensive use of hashing algorithm SHA1 and utilized public crypto systems such as RSA and ElGamal. In addition, Crypto++ provides necessary blocks for generating random safe primes, prime numbers and primitive roots of a cyclic group. In order to generate random polynomials, we applied random number generators for each coefficient to generate n-elements, and then, we applied modular reduction operation to keep the elements in the finite field Z_p. Polynomials were stored as a vector where the first element mapped to the constant term and the last element mapped to the leading coefficient.

Initialization

1. Establish p, q and α, where p and q are large prime numbers such that $p = 2q+1$ and α is a generator of field Z_p^*.
2. Each bidder j generates a public-key from private-key S_j as follows $P_j = \alpha^{S_j} (mod\, p)$.
3. Auctioneer(s) publish the different price choices $\{w_1, ...w_m\}$.

Bid Submission

1. Each bidder chooses random numbers $x, k \in Z_q^*$ and computes $h, r, \tilde{r}, c, s$ based on the following equations:

$$h = \alpha^x (mod\ p)$$
$$r = \alpha^k (mod\ p)$$
$$\tilde{r} = r^x (mod\ p)$$
$$c = Hash(w_k,\ \tilde{r})$$
$$s = k - cS_j (mod\ q)$$

Winner Determination

1. Auctioneer(s) order price list in descending order and select price w_i starting with the highest price w_m.
2. Auctioneer(s) determine, based on the equality or inequality of two discrete logs, if the bidder(s) committed to a price according to the following:

$$u,\ v,\ w\ \in\ Z_q^*$$
$$\tilde{s} = k - (v + w)x(mod\ q)$$
$$\beta = \alpha^s\ P_j^{Hash\ (w_m,\ \tilde{r})}$$
$$\beta^{\tilde{s}}\tilde{r}^{v+w} = \beta^k\ (mod\ q) \quad (equality)$$
$$\beta^{\tilde{s}}\tilde{r}^{v+w} \neq \beta^k\ (mod\ q) \quad (inequality)$$

3. The bidder(s) that committed to the price w_i are the winners. If bidders cannot prove the commitment, the next price from the list is selected and the process reiterated.
4. Once a bidder is found to have commitment to a price w_i, the auctioneer(s) verify the validity with the following equation and conclude the auction:

$$\tilde{r} = (\alpha^s\ P_j^{Hash(w_k,\tilde{r})})^x\ (mod\ p)$$

Fig. 4. Sakurai's and Miyazaki's Protocol.

Our experiments were centered on computational complexity and communication overhead around initialization and verification. For each protocol, we tested initialization based on four distinct modulus sizes: 128-bit, 256-bit, 512-bit and 1024-bit. Verification time was measured by allowing the bidders to have different bidding preferences and by manipulating the number of bidders present during the auction. For instance, we measured verification complexity in scenarios containing 25, 50, 75 and 100 bidders. At the same time, the bidders could choose a bid b_i at random from the whole set if the bidding parameter was 100%, otherwise they would have to choose only from a subset. For example, if the set contained 100 elements in numerical order, then bidding parameter 75% essentially meant the bidders would ignore bidding the top 25 elements, and instead, he would choose a bid b_i at random from the remaining 75 lower order elements. Hereafter, we will refer to this bidding preference, which we tested at 25%, 50%, 75% and 100%, as the *price range* parameter.

For simplicity, the experiments were created using a Command Line Interface and a common graphical user interface. Our computation model was synchronous, thus it introduced some delay. However, the delays introduce by this model was relative. Some modules that were affected by the synchronous model were creation of public/private-key pairs, generation of polynomials and publishing the results to our simulated bulletin board. In terms of our computing power, we conducted our executions using a computer with Intel Core $i74810MQ$ CPU @ 2.80 GHz and 16GB RAM. While running the experiment, we ended every process that would steal computing power from the operating system. Besides, we shut down the network and closed down any ports, i.e., we made the operating system solely focus on running the experiment.

5.1 HK's Protocol Based on Secure MPC

The first set of results correspond to the non-verifiable protocol of [11]. Naturally, the initialization increased with an increase in the modulus size, Figure 5. The first reason for an increase is that generating a random prime number becomes increasingly expensive with a greater bit size, and at best, the algorithms produce only probabilistic prime numbers. The second reason for the observed increase is that, for each polynomial, we chose random numbers based on the size of the field, thus the modular reduction increased and the numbers became larger.

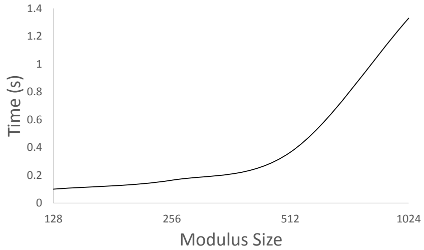

Fig. 5. Initialization of HK's Protocol.

Figure 6 demonstrates the required time for different number of bidders and varying price ranges. The verification seemed to be more affected by the price range and the bidder size rather than the bit size of the modulus. Two factors contributed to the increased in time. First, in this protocol, the private value of the bidder is concealed in the degree of a polynomial meaning that, in order to conceal a bidding value of \$100, we need to construct a polynomial of degree 100, i.e., more computation when evaluating shares and using the addition operation of MPC. Secondly, with increasing price, we need to increase number of auctioneers if it is required to have the same security threshold. However, increasing number of auctioneers increases communication complexity during the sharing and reconstruction parts of the protocol.

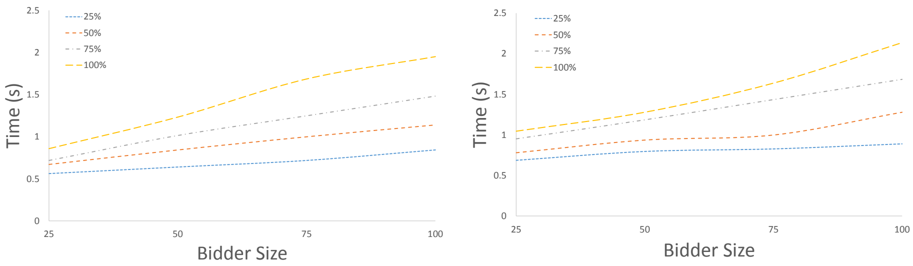

Fig. 6. Verification of HK's Protocol: 128b, 512b.

Figure 7 shows the initialization time for the same protocol when verifiability is introduced as a method to prevent the bidders from repudiation and the auctioneers from casting false bids with the purpose of inflating prices. The result of adding extra layers of robustness is an increase in computation. Unlike the simpler approach, we must generate a prime and two distinct generators of the cyclic group. Also, the bidders must generate two distinct polynomials $f(x)$ and $h(x)$. For every coefficient, each bidder must submit commitments. The auctioneers must verify the submitted commitments before they establish a trust in the bidder. The result is an increase in time not only due to a larger modulus size but also the extra numbers of precautions added to the protocol.

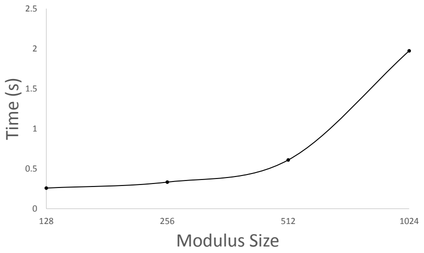

Fig. 7. Initialization of 2nd HK's Protocol.

The same pattern as the simple implementation can be observed in the verifiable protocol, Figure 8. That is, with a larger number of bidders and a greater number of price ranges, we note an increase in time. The extra accumulated time is due to communication complexity and extra verification steps. The auctioneers must publish two constants Y_j and Z_j based on the multiplication computed from $g_1^F g^H$ for each corresponding α_j. As another additional step, the bidders must verify that the auctioneers computed their values correctly.

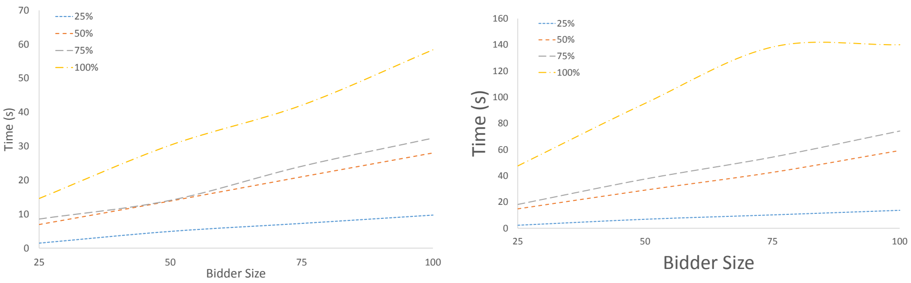

Fig. 8. Verification of 2nd HK's Protocol: 128b, 512b.

5.2 KS's Protocol Based on Pub-Key Encryption

Figure 9 demonstrates the initialization time of [23] for two different implementations using ElGamal and RSA schemes respectively. In both cases, the initialization time rises with modulus sizes as it is expensive to generate large primes. The time for ElGamal is higher than RSA since the prime generation algorithm needs to find prime p for which $(p-1)/2$ is also a safe prime, whereas RSA only requires two large unrelated primes. Clearly, the number of price ranges also affects the total initialization time.

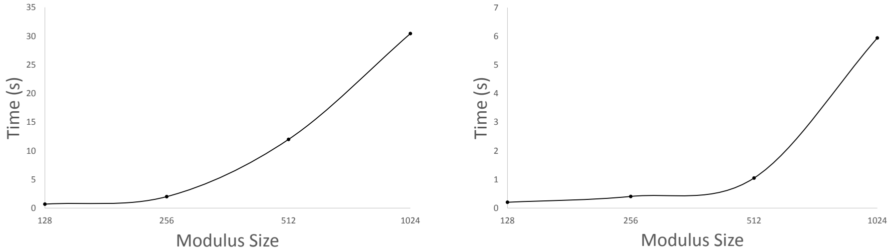

Fig. 9. Initialization of KS's Protocol: ElGamal (left) and RSA (right).

One expected outcome is that, increasing the modulus size increases the computational complexity since we have bigger keys. More subtle, however, is the fact that we observed an increase in verification time for lower price ranges, Figure 10 and Figure 11. We can justify this because of the Dutch-style nature of the auction. When we set the price range to 100% and we have 100 bidders, it is very likely that one of the bidders will bid the highest price. Since decryption occurs from the highest decryption key to lowest, essentially we will greatly reduce the cost if we find a bidder that bids equal to or very close to the highest price. On the other hand, when the price range parameter is set to 25%, the auctioneers lose a significant amount of time decrypting values for which nobody placed a bid. Therefore, for 100 bidders and 100% price range, the result is minimized whereas it is maximized for 100 bidders and 25% price range.

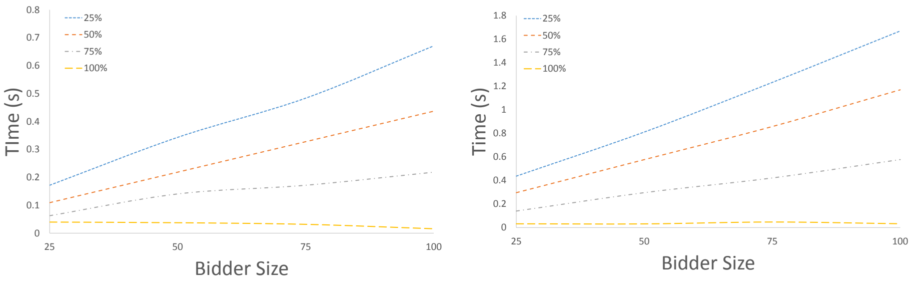

Fig. 10. Verification of KS's Protocol-ElGamal: 128b, 512b.

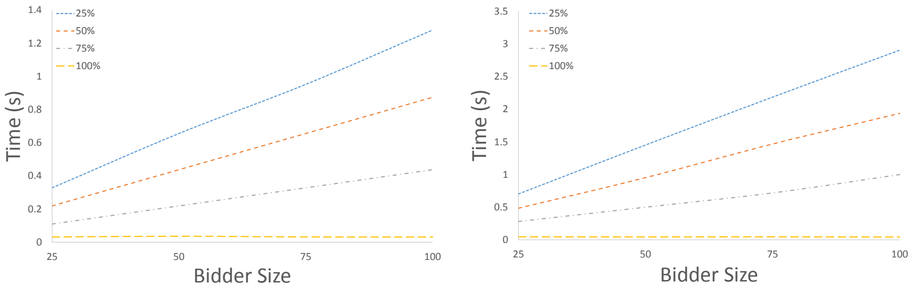

Fig. 11. Verification of KS's Protocol-RSA: 128 & 512 Bits.

Our choice for ElGamal and RSA is due to the fact that these two are well-known public-key encryption schemes. At the end, the verification times were very similar with RSA being a bit slower than ElGamal. Although encryption is faster for ElGamal, RSA has significant advantage during the initialization steps because of a slow prime generation in ElGamal.

5.3 S-&-M's Protocol Based on Commitment

In this section, we examine the protocol proposed in [24]. The first step in the design of the protocol is to generate two primes p and q where $p = 2q + 1$ and α

is a generator. The bidders must compute private and public values. Because no encryption or decryption is required during the initialization phase, this protocol is the fastest to be initialized. Obviously, the complexity increase observed with an increase in the modulus size, shown in Figure 12.

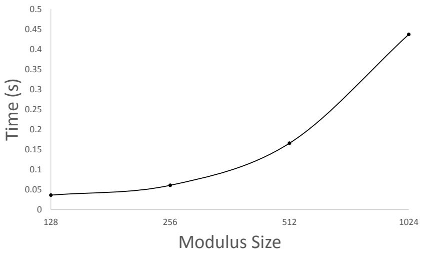

Fig. 12. Initialization of S-&-M's Protocol

During the bidding process, the bidders commit to a bid and attach a digital signature. In the opening phases, the auctioneers start at the highest possible price and receive a proof from each bidder showing equality or inequality. Therefore, the verification time required for the protocol is proportional to the number of bidders and inversely proportional to the price range, as shown in Figure 13.

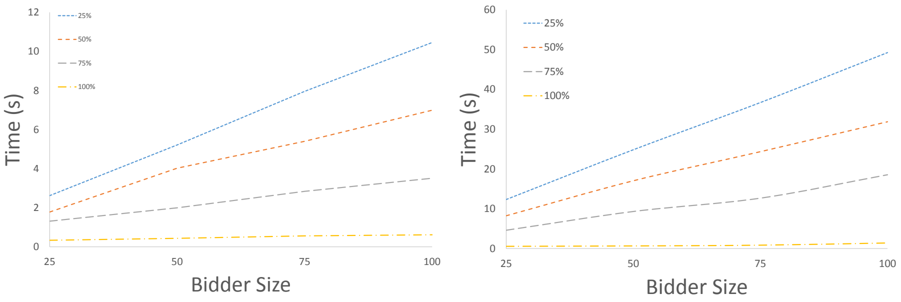

Fig. 13. Verification of S-&-M's Protocol: 128b, 512b.

It appears that the modulus size significantly affects the verification time. To better understand the result, we simply analyze one important step of this protocol specifically when the auctioneers compute $\beta = \alpha^s P_j^{H_i(w_m,r)}(mod\, p)$. In fact, we need to perform hashing and then we have exponentiation of large numbers. Afterward, the auctioneers and bidders execute a protocol for proving equality or inequality of two discrete logs. Since the auction is constructed in a Dutch-style manner, the auctioneers and bidders must exchange information over several rounds before defining the winner. Once a bidder successfully proves the equality of his bid with the current standing price, an extra step is required to prove confirmation. In the confirmation step, the bidder must send the auctioneers his private exponent x in the discrete log, and finally, the auctioneers can confirm if the parameter satisfies $r = (\alpha^s P_j^{H_i(w_m,r)})^x(mod\, p)$.

5.4 Comparing All Three Protocols

In Figure 14 and Figure 15, we provide a unified comparison of all protocols. To fit the entire result in one visible plot, we applied a logarithmic scale for the time axis. For initialization times, we considered 128, 256, 512 and 1024 bits. For verification times, we have plotted 512 bits, 50 bidders, and price range 50%.

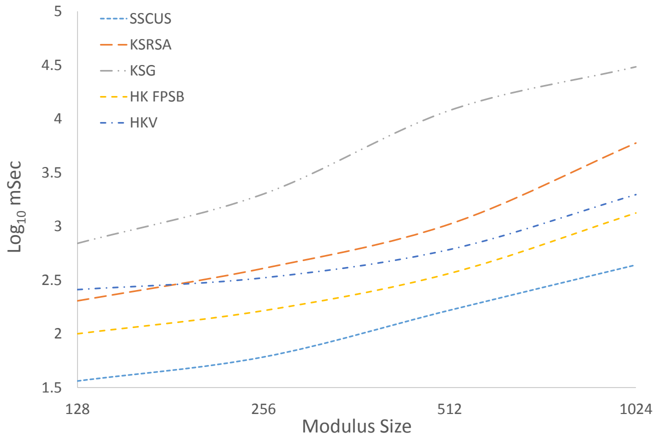

Fig. 14. Initialization Time

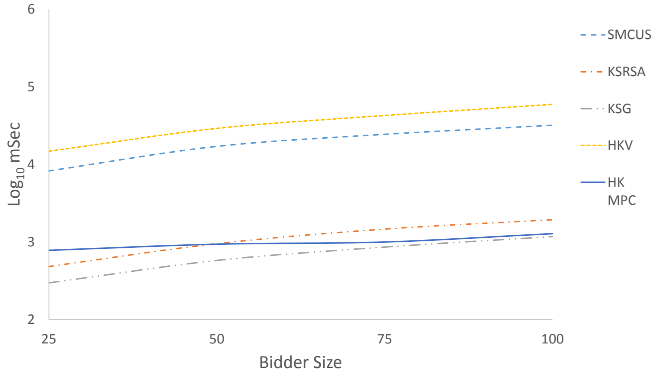

Fig. 15. Verification Time

Within the initialization plot, the KS-ElGamal is the most expensive protocol and the S-&-M is the fastest one. It should be noted that the slow initialization is not that important since preparation of the key-pairs can be performed prior to the auction. Also, if the keys are created in parallel, it would be significantly faster. In the case of verification, the most expensive protocol is the 2nd version of the HK protocol and the fastest is KS-ElGamal. In other words, HK-Verifiable is very expensive since we reconstruct a polynomial using Lagrange interpolation for polynomials with up to 50 terms where each coefficient has around 500 bits. After this protocol is S-&-M since for each round, the determination of equality or inequality requires many calculations and there could be many rounds.

6 Concluding Remarks

We have analyzed five different protocols in the literature of sealed-bid auctions. The protocols consisted of different approaches. Namely, we studied protocols using secure MPC, public-key encryption and commitment scheme. We noticed that protocols using MPC will have a large number of communication rounds. In the case of using public-key encryption schemes, we can encrypt and decrypt bids efficiently, however, we must realize that there is risk of auctioneers opening all bids since they hold all the decrypting keys. Commitment schemes also suffer from communication complexity since, at every round, the bidders must prove that their commitments are not equal to the standing price. In conclusion, a protocol can be fast such as HK and KS, but in order to provide higher security and robustness, such as HK-Verifiable or S-&-M protocols, we must spend extra computation and/or communication rounds. As a part of our future work, we intend to analyze unconditionally secure sealed-bid auction protocols.

Acknowledgements

We gratefully acknowledge our research sponsors, College of Engineering and Computer Science (COECS) and Institute for Sensing and Embedded Network Systems Engineering (I-SENSE) at FAU, for making this research work possible.

References

1. Abe, M., Suzuki, K.: M+ 1-st price auction using homomorphic encryption. In: International Workshop on Public Key Cryptography. pp. 115–124. Springer (2002)
2. Alvarez, R., Nojoumian, M.: Comprehensive survey on privacy-preserving protocols for sealed-bid auctions. Computers & Security (2019). https://doi.org/https://doi.org/10.1016/j.cose.2019.03.023
3. Ben-Or, M., Goldwasser, S., Wigderson, A.: Completeness theorems for non-cryptographic fault-tolerant distributed computation. In: Proceedings of the twentieth annual ACM symposium on Theory of computing. pp. 1–10. ACM (1988)
4. Boyar, J., Chaum, D., Damgård, I., Pedersen, T.: Convertible undeniable signatures. In: Conference on the Theory and Application of Cryptography. pp. 189–205. Springer (1990)
5. Brandt, F.: A verifiable, bidder-resolved auction protocol. In: Proceedings of the 5th International Workshop on Deception, Fraud and Trust in Agent Societies, SI on Privacy and Protection with Multi-Agent Systems. pp. 18–25 (2002)
6. Cachin, C.: Efficient private bidding and auctions with an oblivious third party. In: Proceedings of the 6th ACM conference on Computer and communications security. pp. 120–127. ACM (1999)
7. Franklin, M.K., Reiter, M.K.: Verifiable signature sharing. In: International Conference on the Theory and Applications of Cryptographic Techniques. pp. 50–63. Springer (1995)
8. Franklin, M.K., Reiter, M.K.: The design and implementation of a secure auction service. IEEE Transactions on Software Engineering **22**(5), 302–312 (1996)

9. Fujishima, Y., Leyton-Brown, K., Shoham, Y.: Taming the computational complexity of combinatorial auctions: Optimal and approximate approaches. In: IJCAI. vol. 99, pp. 548–553. DTIC Document (1999)
10. Juels, A., Szydlo, M.: A two-server, sealed-bid auction protocol. In: International Conference on Financial Cryptography. pp. 72–86. Springer (2002)
11. Kikuchi, H.: (m+1) st-price auction protocol. IEICE Trans. on Fundamentals of Electronics, Communications and Computer Sciences **85**(3), 676–683 (2002)
12. Kikuchi, H., Hakavy, M., Tygar, D.: Multi-round anonymous auction protocols. IEICE Transactions on Information and Systems **82**(4), 769–777 (1999)
13. Kikuchi, H., Hotta, S., Abe, K., Nakanishi, S.: Distributed auction servers resolving winner and winning bid without revealing privacy of bids. In: 7th Int. Conf. on Parallel and Distributed Systems. pp. 307–312. IEEE (2000)
14. Krishnamachari, S., Nojoumian, M., Akkaya, K.: Implementation and analysis of dutch-style sealed-bid auctions: Computational vs unconditional security. In: 1st Int. Conf. on Information Systems Security and Privacy. pp. 106–113 (2015)
15. Lipmaa, H., Asokan, N., Niemi, V.: Secure vickrey auctions without threshold trust. In: Int. Conference on Financial Cryptography. pp. 87–101. Springer (2002)
16. Naor, M., Pinkas, B., Sumner, R.: Privacy preserving auctions and mechanism design. In: Proceedings of the 1st ACM conference on Electronic commerce. pp. 129–139. ACM (1999)
17. Nojoumian, M.: Novel Secret Sharing and Commitment Schemes for Cryptographic Applications. Ph.D. thesis, Department of Computer Science, University of Waterloo, Canada (2012)
18. Nojoumian, M., Stinson, D.R.: Unconditionally secure first-price auction protocols using a multicomponent commitment scheme. In: 12th Int. Conf. on Information and Communications Security. LNCS, vol. 6476, pp. 266–280. Springer (2010)
19. Nojoumian, M., Stinson, D.R.: Efficient sealed-bid auction protocols using verifiable secret sharing. In: 10th International Conference on Information Security Practice and Experience. LNCS, vol. 8434, pp. 302–317. Springer (2014)
20. Pedersen, T.P.: Non-interactive and information-theoretic secure verifiable secret sharing (1998)
21. Peng, K., Boyd, C., Dawson, E., Viswanathan, K.: Robust, privacy protecting and publicly verifiable sealed-bid auction. In: International Conference on Information and Communications Security. pp. 147–159. Springer (2002)
22. Rothkopf, M.H., Pekeč, A., Harstad, R.M.: Computationally manageable combinational auctions. Management science **44**(8), 1131–1147 (1998)
23. Sako, K.: An auction protocol which hides bids of losers. In: International Workshop on Public Key Cryptography. pp. 422–432. Springer (2000)
24. Sakurai, K., Miyazaki, S.: A bulletin-board based digital auction scheme with bidding down strategy-towards anonymous electronic bidding without anonymous channels nor trusted centers. In: Proc. International Workshop on Cryptographic Techniques and E-Commerce. pp. 180–187 (1999)
25. Sakurai, Y., Yokoo, M., Kamei, K.: An efficient approximate algorithm for winner determination in combinatorial auctions. In: Proceedings of the 2nd ACM conference on Electronic commerce. pp. 30–37. ACM (2000)
26. Sandholm, T.: Algorithm for optimal winner determination in combinatorial auctions. Artificial intelligence **135**(1-2), 1–54 (2002)
27. Shamir, A.: How to share a secret. Communications of the ACM **22**(11), 612–613 (1979)
28. Suzuki, K., Yokoo, M.: Secure multi-attribute procurement auction. In: Int. Workshop on Information Security Applications. pp. 306–317. Springer (2005)