Anonymous sealed bid auction protocol based on a variant of the Dining Cryptographers' protocol *

Mihály Bárász, Péter Ligeti, László Mérai, Dániel A. Nagy

September 30, 2011

Abstract

Sealed bid auctions are a popular means of high-stakes bidding, as they eliminate the temporal element from the auction process, allowing participants to take less emotional, more thoughtful decisions. In this paper, we propose a digital communication protocol for conducting sealed bid auctions with high stakes, where the anonymity of bids as well as other aspects of fairness must be protected.

The Dining Cryptographers' Protocol (denoted by DC) was presented by David Chaum in 1988. The protocol allows the participants to broadcast a message anonymously. In a recent paper (Another Twist in the Dining Cryptographers' Protocol, submitted to Journal of Cryptology) the authors propose a variant of the original DC eliminating its main disadvantages. In this paper we present a cryptographic protocol realizing anonymous sealed bid auctions, such as first price or Vickrey auction, based on this variant. The proposed scheme allows to identify at least one dishonest participants violating the protocol without the using of Trusted Third Parties. Additionally, we require that bids are binding. It is achieved by enabling all participants acting in concert (the so-called "angry mob") to find out the identity of the winner, in case the winner fails to make the purchase.

*This research was partially supported by the Momentum (Lendület) fund of the Hungarian Academy of Sciences and the European Union and the European Social Fund have provided financial support to the project under the grant agreement no. TÁMOP 4.2.1/B-09/1/KMR-2010-0003.

AMS Classification: 94A60, 68P25
Keywords: sealed bid auctions, anonymous broadcast, dining cryptographers, proof of knowledge

1 Introduction

In a sealed bid auction protocol every participant submits a bid of his choice secretly and anonymously, the goal is to let participants and other observers compare the bids (but only after all bids have been submitted) allowing the winner to prove the fact of winning the auction to anyone of his choosing, without revealing the identities corresponding to the bids. Additionally, we require that bids are binding, i.e. the winner must pay the price of the goods and the protocol satisfy several security definitions which will be specified later in 2.

The most frequently used variation is *first price sealed bid auction* where the highest bid wins and the winner pays the amount of it as well. The strategies of the participants depend on the price they are able to pay and on their estimation of the above participants bids. From the game-theoretic point of view, first price is equivalent to Dutch auction, in the sense that there is a bijection between the sets of strategies of the two auction-type. Other variant is *second price* or *Vickrey auction*, where the highest bid wins but the winner pays the second highest bid only. It is equivalent to English auction.

For the communication between the participants of the auction we use an anonymous broadcast channel, i.e. the Dining Cryptographers' protocol introduced by Chaum [6]. Its purpose is to let a group of communicating parties broadcast messages within the group by letting each party send an encrypted version of their message, which can later be combined in order to decrypt each message without being able to match senders with the decrypted plaintext messages. The idea, using the Dining Cryptographers protocol for e-auctions is due to Stajano and Anderson [17].

It is important to emphasize that our protocol avoids the use of trusted third parties (or TTPs for short), which according to one popular definition are "third parties that can violate security policies and get away with it". Instead, it relies primarily on participants trusting their own devices to execute the protocol as described.

1.1 Related work

Sealed bid auctions

There are other solutions achieving sealed bid auctions in the literature. The first solution using cryptographic tools is due to Franklin and Reiter [9], the main building blocks of their protocol are secret sharing techniques, electronic money and digital signatures. Nakanishi, Fujiwara and Watanabe [11] solved this problem using undeniable signatures and bit-commitment schemes. Chida, Kobayashi and Morita [7] presented a new efficient value-comparing method. It allows two auctioneers to judge whether two values are equal or not without leaking them. Suzuki, Kobayashi and Morita [18] proposed a scheme using hash-chains.

Brandt propose solutions for first and second price auctions in his paper [4]. Basically, the participants are making a "vote" for every possible price (i.e. he allow to pay it or not) from the highest to the lowest one and the first one which has a "yes" ballot is the winner price. The author propose additive secret sharing for masking the ballots.

The protocol of Abe and Suzuki [1] uses chameleon bit-commitments and a group of Trusted Third Parties. Peng, Boyd and Dawson [16] are using homomorphic secret sharing yielding highest level of security. Nakanishi, Yamamoto and Sugiyama [12] proposed two sealed bid auction protocols based on efficient multiparty computation protocols. In a later paper of Brandt [5] homomorphic encryptions are used for constructing the auction protocol. In a recent paper, Nojoumian and Stinson [15] propose three solutions guaranteeing unconditionally secure protocols.

Dining cryptographers network

In the original paper [6] Chaum describes in detail a protocol for broadcasting a single bit anonymously and generalizes it to sequence of bits. One of the biggest deficiencies of the original DC protocol originates exactly from its perfect anonymity. Namely, it can be disrupted by a malicious participant in a way that he learns the message(s) but no other participant does. In his original paper [6], Chaum recognizes the problem and suggests using "traps" combined with slot reservation techniques to avoid this weakness at the cost of multiple broadcast rounds. Several further improvements for this problem are given [2], [10], [19], in this paper we present a recent modification [3] in detail only, because our proposed auction protocol based on this variant.

Our protocol allows to conduct the anonymous auction over a broadcast channel that is not anonymous by having three rounds in which each participant broadcasts a special message. In the end, all bids can be decrypted anonymously and the correctness of the protocol's execution can be verified by each participant. In order to discourage active interference and sabotage, our protocol provides facilities for discovering malformed messages and stripping their senders of anonymity. Small-scale (so-called boardroom) voting and auctions are the most obvious applications of such messaging. Using commodity hardware (e.g. smartphones) and typical communication channels (e.g. WiFi), our protocol does not scale well beyond a few dozen participants, as the time required for its execution is roughly proportional to the square of the number of participants.

2 Security requirements

Here we present the (conventional and generalized) security requirements we want the auction system to satisfy:

1. **Perfect bid anonymity**: this requirement ensures, that knowledge about the partial bids of every set of bidder is only computable by the coalition of all the remaining bidders. (Note that this requirement is stronger than the usual "Anonymity" which is about the 1-element sets of bidders.)

2. **Self verifying**: every participants and outsiders are able to compute the result after the auction procedure without the help of TTP-s.

3. **Universal verifiability**: every bidder and outsider can be convinced that all bids have been taken into comparison of the bids.

4. **Fairness**: no participant has knowledge about the others' bids until fully committed to a bid of their own.

5. **Catching cheaters**: the participants are able to detect and identify at least one dishonest user violating the protocol without the help of TTP-s.

6. **Non-repudiation**: the winner can be identified after the winning bid is opened, when it is necessary (i.e. she/he does not pay for the goods).

7. **Opportunity to keep the transcript**: it is just an option. If necessary, bidders could be able to record their bids and all of their communication in a transcript. It can be used to prove the correctness of the auction to any third party.

8. **Technology independent**: the user only needs to trust the security of the protocol and the correct operation of his own device. Specifically, one need not to rely on the correct operation of the devices of other participants.

9. **Open source, open code**: the security of the system must not rely on the secrecy of the algorithm or the source code of the used programs.

3 Building blocks

We use some cryptographic primitives which are not widely used: an improved Dining Cryptographers' protocol [3] and protocols which proves some partial knowledges [8].

3.1 Dining Cryptographers protocol

The *Dining Cryptographers protocol* allows participants to broadcast their secret messages M_i anonymously, i.e. at the end of the protocol the set $\{M_1, \ldots, M_n\}$ is known by every participant. This protocol will be denoted by $\mathrm{DC}[M_1, \ldots, M_n]$

This protocol is an improvement of the original Dining Cryptographer's protocol proposed in [6] which eliminates the security gaps arising form its strong anonymity properties. Originally Chaum proposed a protocol to allow participants to compute the sum of his own bits anonymously. Namely let b_i ($i \in \{1, \ldots, n\}$) the secret bits of the participants, and let $s_{i,j} = s_{j,i}$ ($i \neq j$) the common secret of the pair (i, j). Then the i-th participant computes and publishes the following sum

$$S_i = \sum_{j \neq i} s_{i,j} + b_i.$$

The sum of the published S_i is

$$\sum_i S_i = \sum_i \sum_j s_{i,j} + b_i = \sum_i b_i.$$

The protocol can be trivially extended to a suitable anonymous broadcast protocol by replacing the group $\mathbb{Z}_2$ to $\mathbb{Z}_m^k$ (where now $s_{i,j} = -s_{j,i}$) and letting the participants to use such a vector instead of bits b_i where all but one coordinate are zeros. However, to prevent participants from using the perfect anonymity of this protocol for cheating further improvements are necessary.

The basic idea in the recent version of the DC protocol [3] is to make additional DC rounds in other communicative groups. First, in *Slot reservation*, the participant reserves his own slot (or coordinate in $\mathbb{Z}_m^k$) using for broadcast communications during the next stages performing classical DC protocol in $\mathbb{Z}_2^K$. The next stage is *Messaging*, when participants broadcast their messages in two steps: first they broadcast a homomorphic function of the message thereof to prevent cheating, then they broadcast the message itself. The last stage is *Investigation*, which is applied only in case of irregularities, when cheaters can be detected and disqualified by the honest participants.

3.2 Proof of knowledge protocols

The *proof of knowledge of a discrete logarithm* protocol allows everyone to prove his knowledge of secret key x for some given public key g^x, without revealing any additional information about the secret key. This protocol will be denoted by $\mathrm{PoK}[x : \ g^x = y]$.

Cramer, Damgård and Schoenmakers [8] proposed a method to prove also some partial knowledge about discrete logarithm. For fixed g, h generators the protocol $\mathrm{PoK}[s : \ g^s = u; \ h^s = v_1 \vee \cdots \vee h^s = v_k]$ allows everyone to prove his knowledge of s such that the following equation holds

$$g^s = u, \quad h^s = v_i$$

for some (i.e. exactly one) $i \in \{1, \ldots, k\}$.

It can be proven in the following way:

1. Let us assume, that the prover knows an s such that $h^s = v_i$. The prover chooses random values $w_1, \ldots, w_k$, $c_1, \ldots, c_{i-1}, c_{i+1}, c_k$ and computes

$$s_j = \begin{cases} g^{w_i} & \text{if } i = j \\ g^{w_j} u^{-c_j} & \text{if } i \neq j \end{cases} \quad \text{and} \quad t_j = \begin{cases} h^{w_i} & \text{if } i = j \\ h^{w_j} v_j^{-c_j} & \text{if } i \neq j. \end{cases}$$

   The prover publishes the commitments $s_1, \ldots, s_k$, $t_1, \ldots, t_k$.

2. The verifier sends a challenge c.

3. The prover chooses c_i such that $c_1 + \cdots + c_k = c$. Then the prover publishes the certifications $c_1, \ldots, c_k$ and $r_1, \ldots, r_k$ where

$$r_j = \begin{cases} w_i + c_i s & \text{if } i = j \\ w_j & \text{if } i \neq j. \end{cases}$$

4. The certifications are correct, if the following equations hold:

$$g^{r_j} = s_j u^{c_j}, \quad h^{r_j} = t_j v_j^{c_j} \quad \text{for } j = 1, \ldots, k.$$

4 The Auction protocol

Let n denote the number of participants, let p be a large enough prime and q a prime such that $q|p-1$ holds. Let $\mathbb{Z}_q \cong G \leq \mathbb{Z}_p^*$ such that the Diffie-Hellman assumption holds in G and g be a generator of G.

The proposed protocol consists of two stages. The first one is *Auction*, when the participants broadcast their bids using the Dining Cryptographer's protocol. The next one is so-called *Angry Mob* stage in which the participants are able to identify the winner when he does not pay for the goods.

Auction

Denote by $P_i \in \{0,1\}^c$ the bid of the participant i (here we suppose that every acceptable price can be encoded in c bits). The i-th participant chooses a random secret b_i, computes his "fingerprint" g^{b_i} and the message

$$M_i = P_i \| g^{b_i}.$$

Now the participants perform the Dining Cryptographers protocol for these messages, i.e. $\mathrm{DC}[M_1, \ldots, M_n]$.

Angry Mob

This stage is necessary only if the winner doesn't pay the goods and provide a protocol to the honest participants to prove that their fingerprint does not belong to the set of dishonest participants' fingerprints without revealing which fingerprint belongs to which honest participant.

Let $M = P \| g^b$ be the winner's bid and let $\Gamma = \{g^{b_i} : \ i = 1, \ldots, n\} \setminus \{g^b\}$ the set of honest participant's fingerprints. Then the protocol consists of $n-1$ rounds where in the i-th round the i-th participant proves his honesty by an interactive proof. Let h be a generator and let $\Gamma_i = \{h^{b_j} : \ b_j \in B, \ j = i, \ldots, k\}$. (Let us note, that in the case $i = 1$ we have $h = g$.)

1. The i-th participant shuffles Γ_i by a randomly chosen s

$$\Gamma_i^s = \{h^{sb_j} : \ b_j \in B, \ j = i, \ldots, k\}$$

   and computes $v = h^s$. Then he publishes h, v and Γ_i^s (where now we denote the elements of Γ_i^s by $\Gamma_i^s = \{y_i, \ldots, y_k\}$).

2. Next, the i-th participant proves the correctness of the shuffle performing the protocols

$$\text{PoK}[s : \ h^s = v; \ x^s = y_i \vee \cdots \vee x^s = y_k], \quad x \in \Gamma_i.$$

3. The i-th participant proves his honesty by performing $\text{PoK}[x : \ v^x = y_i]$

4. Finally the participants replace h by h^s, and define Γ_{i+1} by $\Gamma_i^s \setminus \{y_i\}$

Clearly, the participant who cannot prove his honesty must be the winner.

5 Security analysis

Let us mention, that most of the security requirements of a sealed bid auction have to satisfy are very similar to the requirements of a boardroom voting system, hence one can prove them with similar to the methods presented in [3]. The only one additional requirement is non-repudiation and we fulfill this criterion with the help of the angry mob protocol. Then if we suppose that a malicious participant can cheat in the angry mob protocol, i.e. she can perform a proof of knowledge of whether a discrete logarithm or a partial knowledge of discrete logarithm such that she doesn't have the corresponding secret value, we have a contradiction. More details on the security of that protocols can be found in [8].

6 Conclusions

We have presented a digital auction protocol consisting of two distinct parts: a variant of DC and in case of dispute an "Angry Mob" protocol for collectively discovering cheaters. Both of these building blocks can have applications beyond the presented auction protocol.

The main contribution is the extensive use of a cyclic group in which the D-H problem is hard for a communication protocol based on Dining Cryptographers. While the anonymity of DC is unconditionally true in any cyclic group, various other security properties can be achieved by presenting the attacker with a computationally infeasible problem, if we can operate both directly on indices and their homomorphic images.

This insight allowed us to devise protocols in which only the necessary information is revealed to participants. In particular, we can

- verify that participants broadcast only in their allotted slot without revealing sensitive information about their message and
- prove "innocence" in case the winner of the auction fails to buy without revealing the innocent participants' bids.

An application of the presented "Angry Mob" protocol for a different purpose could be a simple verifiable shuffle similar to that proposed by Andrew Neff [13, 14]. In any application where the shuffle primitive is needed, our protocol can be used directly.

References

[1] Abe, M., Suzuki, K.: Receipt-Free Sealed-Bid Auction. Proceedings of ISC '02, (2002) 191–199

[2] von Ahn, L., Bortz, A., Hopper N., J.: k-anonymous message transmission, in CCS '03: Proceedings of the 10th ACM conference on Computer and communications security, (2003), pp. 122–130.

[3] Bárász, M., Ligeti, P., Mérai, L., Nagy, D.A.: Another Twist in the Dining Cryptographers' Protocol. Submitted to Journal of Cryptology

[4] Brandt, F.: Secure and Private Auctions without Auctioneers, Technical Report FKI-245-02 (2002)

[5] Brandt, F.: How to obtain full privacy in auctions, International Journal of Information Security, **5** (4) (2006) 201–216

[6] Chaum, D.: The Dining Cryptographers Problem: Unconditional Sender and Recipient Untraceability. Journal of Cryptology **1** (1) (1988) 65–75

[7] Chida, K., Kobayashi, K., Morita, H.: Efficient Sealed-Bid Auctions for Massive Numbers of Bidders with Lump Comparison. Proceedings of ISC '01, (2001) 408–419

[8] Cramer, R., Damgård, I., Schoenmakers, B.: Proofs of partial knowledge and simplified design of witness hiding protocols. CWI Quarterly 8 (1995), **2**, 111–127.

[9] Franklin, M. K., Reiter, M. K.: The design and implementation of a secure auction service, IEEE Transactions on Software Engineering, **22** (1996), 302–312

[10] Golle, P., Juels A.: Dining cryptographers revisited, in Proceedings of Eurocrypt 2004, ser. Lecture Notes in Computer Science, vol. **3027** (2004), pp. 456–473.

[11] Nakanishi, T., Fujiwara, T., Watanabe, H.: An Anonymous Bidding Protocol without Any Reliable Center. Trans. IPS. Japan **41** (8) (2000) 2161–2169

[12] Nakanishi, T., Yamamoto, D., Sugiyama, Y.: Sealed-Bid Auctions with Efficient Bids. Proceedings of ICISC 2003, Lecture Notes in Computer Science **2971** (2004) 230–244

[13] Neff, C. A.: A verifiable secret shuffle and its application to e-voting, Proceedings of ACM CCS 2001, pp. 116–125.

[14] Neff, C. A.: Verifiable Mixing (Shuffling) of ElGamal Pairs, VoteHere document, 2004
`http://votehere.net/vhti/documentation/egshuf-2.0.3638.pdf`

[15] Nojoumian, M., Stinson, D. R.: Unconditionally Secure First-Price Auction Protocols Using a Multicomponent Commitment Scheme, In Proceedings of ICICS'2010. (2010) 266–280.

[16] Peng K., Boyd C., Dawson, E.: Optimization of Electronic First-Bid Sealed-Bid Auction Based on Homomorphic Secret Sharing, Progress in Cryptology – Mycrypt 2005, LNCS 3715 (2005) 84–98.

[17] Stajano, F., Anderson R.J.: The Cocaine Auction Protocol: On the Power of Anonymous Broadcast. Proceedings of IH '99, Lecture Notes in Computer Science **1768** (1999) 434–447

[18] Suzuki, K., Kobayashi, K., Morita, H.: Efficient Sealed-bid Auction using Hash Chain. Proceedings of ICISC '00, (2001) 183–191

[19] Waidner, M., Pfitzmann, B., The dining cryptographers in the disco - underconditional sender and recipient untraceability with computationally secure serviceability (abstract)," in Proceedings of Eurocrypt 1989, ser. Lecture Notes in Computer Science, vol. **434** (1989), pp. 690.

The e-mail adresses of the authors in alphabetical order: `klao@cs.elte.hu`, `turul@cs.elte.hu`, `merai@renyi.hu`, `nagydani@epointsystem.org`.