An Efficient Protocol for eAuction

Jan Seruga and Brian Curtis ACU, Sydney Australia,
Josef Pieprzyk, Macquarie University, Sydney, Australia,

Summary
A secure protocol for electronic, sealed-bid, single item auctions is presented. The protocol caters to both first and second price (Vickrey) auctions and provides full price flexibility. Both computational and communication cost are linear with the number of bidders and utilize only standard cryptographic primitives. The protocol strictly divides knowledge of the bidder's identity and their actual bids between, respectively, a registration authority and an auctioneer, who are assumed not to collude but may be separately corrupt. This assures strong bidder-anonymity, though only weak bid privacy. The protocol is structured in two phases, each involving only off-line communication. Registration, requiring the use of the public key infrastructure, is simultaneous with hash-sealed bid-commitment and generates a receipt to the bidder containing a pseudonym. This phase is followed by encrypted bid-submission. Both phases involve the registration authority acting as a communication conduit but the actual message size is quite small. It is argued that this structure guarantees non-repudiation by both the winner and the auctioneer. Second price correctness is enforced either by observing the absence of registration of the claimed second-price bid or, where registered but lower than the actual second price, is subject to cooperation by the second price bidder – presumably motivated through self-interest. The use of the registration authority in other contexts is also considered with a view to developing an architecture for efficient secure multiparty transactions.

Key words:
eAuction, multiparty security, protocol, trusted-third-party.

1. Introduction

In the realm of single item auctions, the style most familiar to the public is the English or "open-outcry ascending" [4]. This style of auction is conducted in a public forum and consists of bidders proffering successively higher bids until only one remains, who wins the article at the final price. This type of auction is approximated by the mechanism used by eBay.
The open-outcry descending auction works in exactly the opposite way: the auctioneer starts at a very high price, and then lowers the price continuously. The first bidder who calls out that she will accept the current price wins the object at that price. Auction theorists often refer to this as a Dutch auction
(from tulip sales).
A auction form quite suited to electronic implementation is the sealed-bid auction in which each bidder independently submits a single bid without knowledge of others' bids. The article is sold to the bidder who submitted the highest bid. Sealed-bid auctions come in two major forms, characterized by the price paid for the article by the winning bidder. In a first-price sealed-bid auction the winner pays their bid. In a second-price sealed-bid auction the winner pays is the second-highest bidder's bid, or ''second price''. (This auction is sometimes called, by economists, a Vickrey auction after William Vickrey, who wrote the seminal,1961 paper on auction theory).
Klemperer [4] details a general strategic equivalence between descending open-outcry and first-price sealed-bid auctions for single item sales. Strategic equivalence here refers to the buyer's available strategies in a game-theoretic sense. Similarly he details a conditional strategic equivalence between ascending and second-price sealed-bid auctions. These equivalences have led to the terms first-price and second-price being used to refer to both sealed-bid and open-outcry auctions. As such, electronic protocols based on sealed-bid auctions (both first and second price) should provide the same range of strategic options as protocols based on approximations of open-outcry forms.
The following is concerned with electronic protocols for sealed-bid auctions of single items. The properties that are desirable are described followed by an example from the literature. A new protocol is then proposed that provides a significant simplification of this example protocol while preserving many of its useful properties.

2. Desired Sealed-Bid Auction Protocol Properties

Below, following [2], are described ten properties that may be desired by any electronic protocol implementing a sealed-bid auction. The first three are required in that the mechanism would fail to provide an appropriate outcome should they be violated. The remaining seven are desirable but may not all be compatible for a given mechanism. For example, public-verifiability may be incompatible with bid-privacy.

Correctness: The correct winning price and winner is determined according to the auction rules, assuming every

Manuscript received August 5, 2010
Manuscript revised August 20, 2010

party acts honestly. This property is obviously mandatory, but the robustness (see below) of a protocol would be judged by its ability to deal with dishonest participants.
Bid-Confidentiality: Bids are not revealed to any bidder, or to the auctioneer, until the close of the auction.

Fairness: Bids are submitted in ignorance of other bids, they are immutable and may not be repudiated.

Bidder-Anonymity: The identity of losing bidders is never disclosed.

Bid-Privacy: No losing bids value is ever disclosed, even to the auctioneer.

Public-Verifiability: The auction outcome is verifiable by anyone.

Robustness: Corrupt behavior by any participant cannot produce an incorrect outcome.

Price-Flexibility: Any value within a range may be bid – as distinct from many schemes which specify a limited number of potential biddable values.

Rule-Flexibility: The protocol is independent of the auction rules (e.g. first or second price).

Efficiency: Ideally any protocol would be of low computation and communication cost. Indeed the best case would be linear with the number of participants though this is not achieved in most protocols in the literature.

3. The "Untraceable" Protocol

This scheme [2] attempts to provide relative privacy, i.e. the anonymity of the losing bidders is preserved but the actual losing bids do not necessarily remain private.
The scheme relies on the use of separate Registration Authority [RA] that, at the commencement of the auction, issues pseudonyms to each of the registering bidders (who identify themselves using PKI). Bids are then submitted to the auctioneer through an anonymous channel.
To avoid repudiation by the winner a bid privacy recovery mechanism is introduced. Should the winner repudiate, all losing bidders are required to prove their innocence using a "1 out of N" verification protocol. The bidder remaining is therefore the repudiating winner and may be identified by consultation with the RA. Knowledge of the existence of this mechanism allows the protocol to be considered optimistic.
This scheme anonymity (relative privacy) but not absolute privacy but does so at a computational cost that is O(n2) with the number of bidders. In particular the mechanism to identify the repudiating bidder is cumbersome in that it requires the cooperation of all the losing bidders. Below, we present an alternative protocol that obviates these disadvantages.

4. Proposed Protocol

We split the responsibility of the auction between the auctioneer, A, and a registration authority R. A will need knowledge of the actual bids in order to apply the auction rule, but will not need the identity of the bidders. R will need to know the bidders identity but not the actual bids. To preserve bidder anonymity from A, bidders communicate only with R who will in turn communicate with them and A.
A principle difficulty of eAuctions concerns repudiation, either by the bidder or the Auctioneer. To avoid this, the protocol provides receipts to the bidders (similar to certified email) and requires appropriately signed messages to R and A.
We use the two phase commitment / bidding structure based on submission of a bid hash as discussed in [2]. We also make use of a trusted third party (TTP) R as in [1] but used as a registration authority. Instead of the bidder sending his bid hash directly to A, it is sent to the R who associates it with a pseudonym for the bidder.
Note that the use of the TTP differs from that in [3] in that their protocol is optimistic and does not necessarily involve the TTP except where a bidder cheats. We justify the mandatory use of a TTP by noting the simplicity of the cryptographic primitives used and the very limited overhead actually placed on the TTP.

Notation

S, R The sender S and recipient R of a message. Also used as their "identity"
$P \rightarrow Q$ *P* sends to *Q* via a non-secure channel (eg email)
$P \Rightarrow Q$ *P* sends to *Q* via a secure channel (eg SSL or encrypted email)
*Q*c, *Q*p The private (Confidential) and public (Published) keys of *Q*
E(k, m) The asymmetric Encryption of the message m using the key k.
Here we assume: m = **E**(*Q*c, **E**(*Q*p, m)) = **E**(*Q*p, **E**(*Q*c, m))
C(k, m) The symmetric enCryption of the clear message m using the key k
D(k, e) The symmetric Decryption of the encrypted message e using the key k.
We simply assume: m = **D**(k, **C**(k, m))

H(m) A digest (Hash) of the message m.
[m | n] The unambiguous concatenation of message components m and n.
Note that as there is no specific notation given for digital signatures. Although a digital signature is not "Encryption with a private key", the obverse does hold for RSA and simplifies the discussion somewhat.

Phase 1: Registration and Bid Commitment

Using an agreed one-way collision-resistant hash function, **H**, each bidder *B* signs a digest, h = **H**(b) of their bid, b, and registers it with the authority *R*

$B \rightarrow R$ [*B* | h | **E**(*B*c, h)] **1.1**

This message would need to be sent over a secure channel only if bidder anonymity is to be preserved from possible interception. However, it contains no other useful information.

R verifies the identity of *B* using the PKI checks the signature:

h ?= **E** (*B*p, **E** (*B*c, h))

It then generates a pseudonym for *B*, *P*, unique in the auction. This pseudonym, together with the original registration message must be remembered by *R* both to identify the winning bidder at completion and to assist in possible conflict resolution.

R signs the pseudonym and bid hash and sends it to *B* as a registration receipt. This must be sent over a secure channel to maintain B's anonymity from possible interception.

$R \Rightarrow B$ **E**(*B*p, **E** (*R*c, [*P* | h])) **1.2**

B then checks that the receipt matches his bid hash and extracts his pseudonym.

Phase 2: Bid Submission

In order that *B* retain anonymity to the auctioneer, *A*, he communicates his actual bid via the registration authority *R*. Conversely, in order to keep his bid secure from *R*, *B* encrypts it with the public key of the *A:* c = **E** (*A*p, b).

B sends the signed encrypted bid to the authority.
$B \rightarrow R$ [*P* | c | **E** (*B*c, c)] **2.1**

In order that *B* may have a record of his bid, *R* computes a receipt simply by signing the encrypted bid: r = **E** (*R*c, c)
R will send the encrypted bid, c, to *A* but to avert premature bid knowledge by *A*, *R* must further symmetrically encrypt all bids with a common auction key k. Note that *R* has no way of checking that the bid matches the pre-registered value so the auctioneer is enabled to do this by including the original hash in this message.

R then <u>simultaneously</u> sends:

$R \rightarrow B$ [c | r] **2.2**
$R \rightarrow A$ **C**(k, [*P* | c | h]) **2.3**

In principle, *B* now has a receipt if and only if *A* has an encrypted bid

The simultaneous transmission of a message and a receipt echoes that used by Abadi et al [1] in the context of certified email delivery, and suffers from the same potential flaws. Specifically, assuming honesty by *R* (**R** does not corruptly ignore bids) there may be a simple communications failure preventing timely delivery of either component. While *B* can recover their receipt by request (should this be necessary), if *A* does not receive the bid by auction closure, she would not be aware of its absence and could be falsely accused of corruptly ignoring it. To avert the possibility of such ignorance, we require R to provide further information at auction closure, either some sought of checksum or even a simple count of the number of submitted bids. In the unlikely event of a mismatch, *A* could simply request retransmission of all encrypted bids. More complex schemes limiting retransmission requests to specific bids are possible but impose additional overheads that would rarely be justified.

Completion

The auction is closed and *R* may now send the auction key, k, to *A* along with a count of the submitted bids, n.
$R \rightarrow A$ [k | n] **3.1**

If the number of bids received by A is less than n, A will request retransmission of all the encrypted bids from R (it would presumably wait for a timeout period). Note that A can gain no further knowledge over that which R has already attempted to send. In particular, since the auction is closed, no further bids may be corruptly elicited by A based on her knowledge of the extant bids.

A may now decrypt each of the bids.

[*P* | c | h] = **D**(k, [*P* | c | h])
b = E(*A*c, c)

A may now apply the auction rule to determine the winning bidder [*P*', b', h'].
It must of course check that the bid was as registered: h' ?= **H**(b')
P' is of course a pseudonym and *A* must determine the bidders actual identity by consulting *R*.

$A \rightarrow R$ [*P*' | b']

R should perform its own check that **H**(b') = h' as stored, prior to informing both the winning bidder and the auctioneer by simultaneously sending:

$R \rightarrow B'$ success (or second price information)
$R \rightarrow A$ *B*'

Furthermore the actual result must in some way be published although the winners' identity may not be. One way would be for *R* to send a message to all bidders informing them of the winning bid and price.

Security Analysis

Below are considered the major security issues. For this purpose, the auctioneer and the registration authority are presumed not to collude, though they may be separately corrupt. Below we consider the major corruptions that can occur in the execution of an auction.

1) The winner *B* attempts to repudiate his bid b.

From phase I, R has retained *B* 's signature on the bid:
[*B* | h | **E**(*B*c, h)]
This can be used as evidence iff h = **H**(b')

Note that *A* will rely on *R*.

From 2.1 R has also retained the signed encrypted bid of *B*, [*P* | c | **E** (*B*c, c)] and could determine if c ?= **E** (*A*p, b').

2) The auctioneer attempts to repudiate/ignore an otherwise winning bid (*B*, b).

Since the "winning" bid has been published as b', *B* is in a position to know that b > b' and may sensibly lodge a challenge.

B has a receipt signed by *R*: [c | **E**(*R*c, c))] where c = **E** (*A*p, b)

His knowledge of b allows him to show c = **E** (*A*p, b) and that b > b'.

Note that *B* need not rely on *R* for this challenge. However should he not wish to publicly disclose his identity he can simply submit his actual bid to R for the latter to adjudicate.

3) In a second price auction, the auctioneer uses/invents a lower second bid.

Here we rely on the self interest of the actual second-price bidder to prove, as above, that his bid is higher than the published second-price. This would not entail the public disclosure of identity but will require the disclosure of his bid to *R*. Should R not comply he can still prove his bid by his submission receipt.

4) In a second price auction, the auctioneer invents a higher second bid b".

This is resolved by *R* as the bid will simply not be registered and submitted.
Lack of registration is easy to show: there is no **H**(b") in the registry.
Lack of submission requires failure to find **E** (*A*p, b") in the submissions.
This determination should be done as a matter of course with the implication that R will ultimately gain knowledge not only of the winners identity and bid, but also that of the second highest bidder (under a Vickrey auction rule)

It is conceivable that the auctioneer could perform a brute-force search on the hash function looking for non-submitted bids whose hash collides with a submitted bid. If this is a serious possibility, a random number could be appended to bids and this number required to be disclosed along with the second price value.

5) The registration authority fails to provide the winners identity at completion.

To prevent this we could require that *R* sign the bids submitted to *A* (2.2) who could then prove lack of cooperation.

6) A specific bidder is ignored / excluded.

A has no knowledge of bidder identity (except if provided by a bidder via a separate channel) so is unable to exclude

bidders. However *R* could be corrupted to ignore bids from specific bidders. This is a problem common to the use of a TTP.

5. Conclusion and Further Work

We have presented a simple eAuction scheme that appears immune from most corruptions and trades off the use of simple cryptographic primitives with the invocation of a TTP which is required to maintain state. It may now be evaluated in terms of the above listed ten properties.

The three mandatory and one optional properties are satisfied. **Correctness** is guaranteed by the auctioneer acting honestly. **Bid-Confidentiality** if maintained by use of a common auction key in **2.3**, its postponed provision to the auctioneer until the close of the auction at **3.1** and the encryption of the bids using her private key. **Fairness** follows from a combination of bid-confidentiality, the prevention, by the registrant, of multiple (overriding) bids and the above argued non-repudeability of bids. Also, as no set prices are required it is **Price-Flexible**.

Two desired properties are not met. **Bid-Privacy** is only weak in that the auctioneer has access to all bids and could corruptly use this information in the future or provide it to the seller. Similarly **Public-Verifiability** is not provided as only the auctioneer has access to these bids.

Certain desired properties are largely met. Though not fully **Rule-Flexible**, it does cater to the two major types of sealed-bid auctions (or even nth price with a loss of robustness). As knowledge of the bidders' identity is restricted to the registrant, **Bidder-Anonymity** is dependant solely on its propriety. By inspection, the communication and computation cost is linear with the number of bidder so it meets a basic **Efficiency** criteria and, in particular, is scaleable. Finally, as agued above, it is exhibits reasonable **Robustness** in the face of a number of potential corruptions, short of collusion between the auctioneer and the registrant or the registrant unilaterally ignoring bidders.

Further work will focus on improving the efficiency and the possibility of public-verifiability (with the probable total abandonment of bid-privacy). In particular, the round complexity could be reduced by collapsing the registration and bidding phases into one and makes use of the postponed transmission of an auction key in **3.1**.

References

[1] Abadi, M. and Glew, N. 2002. Certified email with a light on-line trusted third party: design and implementation. In Proceedings of the 11th international Conference on World Wide Web (Honolulu, Hawaii, USA, May 07 - 11, 2002). WWW '02. ACM Press, New York, NY, 387-395.

[2] Peng, K., Boyd, C., Dawson, E., and Viswanathan, K. 2003. Five sealed-bid auction models. In Proceedings of the Australasian information Security Workshop Conference on ACSW Frontiers 2003 - Volume 21 (Adelaide, Australia). C. Johnson, P. Montague, and C. Steketee, Eds. ACM International Conference Proceeding Series, vol. 34. Australian Computer Society, Darlinghurst, Australia, 77-86.

[3] Watanabe, Y. and Imai, H. 2000. Reducing the round complexity of a sealed-bid auction protocol with an off-line TTP. In Proceedings of the 7th ACM Conference on Computer and Communications Security (Athens, Greece, November 01 - 04, 2000). P. Samarati, Ed. CCS '00. ACM Press, New York, NY, 80-86.

[4] Klemperer, P. 2004. Auctions: Theory and Practice The Toulouse Lectures in Economics, Princeton University Press, 2004. online at http://www.paulklemperer.org