An Asynchronous and Secure Ascending Peer-to-Peer Auction

Daniel Rolli
Institute of Information Engineering and Management
University of Karlsruhe, Germany
rolli@iw.uka.de

Michael Conrad
Institute of Telematics
University of Karlsruhe, Germany
conrad@tm.uka.de

Dirk Neumann
Institute of Information Engineering and Management
University of Karlsruhe, Germany
neumann@iw.uka.de

Christoph Sorge
Institute of Telematics
University of Karlsruhe, Germany
sorge@tm.uka.de

ABSTRACT

In recent years, auctions have become a very popular price discovery mechanism. Among them, second-price auctions are of theoretical importance, as they have the simple dominant strategy of bidding ones true valuation. Sellers, however, are reluctant to do so, as a malicious auctioneer could take advantage of this knowledge. Several distributed auction mechanisms have been suggested that make it possible to determine the auction outcome without revealing the winner's valuation of the good; however, they are only suitable for sealed-bid auctions.

This paper suggests a distributed mechanism for ascending second price auctions. The auction protocol has the ability to preserve the privacy of the winning bidder's true valuation or highest bid, respectively, with a high probability. The auction protocol is based on a high number of auctioneers that are distributed to several groups. A bidder generates an encrypted chain of monotonously increasing bidding steps, where each bidding step can be decrypted by a different auctioneer group reducing the possibilities of manipulation for malicious auctioneers. Another fundamental advantage of this secure approach is that bidders need not be online except for submitting their bid chain to the auctioneers.

Categories and Subject Descriptors

H.1 [**Models and Principles**]: General; J.4 [**Social and Behavioral Sciences**]: Economics; K.4.1 [**Public Policy Issues**]: Privacy

This work is supported in part by the German Federal Ministry of Education and Research in the reserach program Internet Economics.

SIGCOMM'05 Workshops, August 22–26, 2005, Philadelphia, PA, USA.

General Terms

Algorithms, Economics, Security

Keywords

Distributed Auctions, Privacy, Trust, Security Protocols, Peer-to-Peer Systems

1. INTRODUCTION

Since the beginning of the Internet revolution, auctions have become very popular as a price discovery mechanism. As there are myriads of different auction formats, all of them being different in their ability to set incentives for the bidders, the designer is frequently exposed to the question of which auction format to use.

Basically, there are two classes of auctions: sealed and iterative auctions. In sealed auctions, no information about the competing agents' bids is revealed during the bidding process. Typically, only one bid is submitted by each bidder. Iterative auctions, however, allow for repeated submission of bids by individual bidders. They reveal information about bids of the competing agents and, therefore, allow the agents to adapt their following bids based on the posted information. Either auction type has its advantages as well as disadvantages. While iterative auctions provide valuable information about the other agents' valuations and ideally spur competition or even subjective excitement, they may foster collusion among the involved parties. [13]

Sealed auctions - with a trusted auctioneer or protocol - do not offer information, but allow privacy among bidders and thus decrease the possibilities for collusion considerably.

The most prominent sealed auction format is the so-called Vickrey auction. In essence, it is a sealed auction, where the highest bidder is awarded with the item and pays the second-highest bid as price. Due to this second-price property, the auction is incentive-compatible in a way that truthful revelation of information is a dominant strategy. Regardless of what the other agents bid, it is always preferable to bid the own valuation. In subsequent work, the Vickrey auction has

been generalized to multi-unit settings, where agents can express super-additive preferences. Despite its nice properties, the Vickrey auction has only very rarely been employed in real auction systems. The deficits are commonly ascribed to (1) its vulnerability against an untruthful auctioneer and (2) the reluctance of the bidders to truthfully reveal their private information [14], [11]. Brandt [3] has presented a cryptographic approach to remedy both shortcomings. Additionally, this approach proposes a way to decentralize the auction mechanism. This way, the dependency on a central auctioneer is overcome in some respects, increasing privacy and security of the auction process.

Despite these desirable properties, the decentralized, cryptographic Vickrey auction has a major drawback for many settings - the missing information feedback. If preferences are affiliated, iterative auctions (e.g. ascending auctions) are better off in terms of revenue than sealed auctions. Not surprisingly, most of the auction formats used in the Internet are ascending auctions. Ascending auctions (e.g. on eBay) are often coupled with proxy agents. The proxy agents bid on behalf of the corresponding participants one increment above the preceding highest price, as long as the bid that is given to the proxy agent is at least an increment higher than the current price. The incorporation of a proxy agent projects the second-price property onto iterative auctions and has the theoretically nice effect that the outcome is in the core. That means no coalition can identify a feasible outcome that strictly increases all agents' payoffs (coalition-proof). Additionally, the proxy agent allows participants to take part in the auction without being online at all times. It does, moreover, not diminish the entertainment of ascending auctions. Standard ascending auctions, however, remain vulnerable to DoS attacks.

In this respect Brandt [4] proposes to use the cryptographic approach for iterative auctions as well. Although his approach is partially suited for sealed auctions, it embodies certain disadvantages that make the approach untenable for a use in the Internet [10]. The approach does not allow an asynchronous, but a round-wise bidding procedure. At the end of a round, all participating agents must be online to decrypt the bids. Obviously, this approach cannot represent an asynchronous ascending proxy auction. The paper at hand, though, fills the need of an asynchronous, decentralized auction mechanism by suggesting an alternative cryptographic protocol for ascending proxy auctions. The auctions take place in a P2P network. A large number of nodes are available and able to act as auctioneers.

The remainder of this paper is structured as follows: Firstly, literature is reviewed, and the requirements of an ascending proxy auction are pointed out. Subsequently, the protocol for the auction is presented. The paper concludes with a summary and future work.

2. RELATED WORK

In recent years, a couple of cryptographic protocols have been proposed for auctions. Among the first, Franklin and Reiter developed a secure sealed auction protocol [7]. Their protocol, however, does not achieve privacy preservation once the auction is resolved. Privacy preservation means that neither bids nor bidder identities are revealed. Since privacy preservation apparently is a very important requirement for sealed auctions, various new protocols were suggested to remedy this shortcoming [3].

Among those newly suggested approaches, only few can cope with auction formats that both comply with the privacy preservation requirement and embody other pricing rules than pay-your-bid. In particular, only few formats currently support a secure Vickrey auction [15].

The auction protocols that satisfy privacy preservation and also support more sophisticated pricing schemes can be classified as follows. [1]

- *Distributed computation among multiple auctioneers:* In a first class, the agents submit shares of the bids to different auctioneers. The auctioneers jointly compute the auction price by using the techniques of secure multiparty function evaluation. The gist of those techniques is marked by auctioneers that compute the auction price without knowing any bid [9], [8].

- *Partially trusted third party:* The second class of protocols requires the introduction of a third party, which controls the auctioneer. Crucial for those protocols is that the third party need not be fully trusted but can draw on a weaker form of trust. [1],[5]

Both classes inherently impose several challenges and problems. In fact, the first class requires a threshold number of obedient auctioneers. Otherwise, collusion among malicious auctioneers may occur. The second class of protocols requires some sort of third party that is trustworthy to a certain degree.

Besides, all current approaches only support sealed or round-wise iterative auctions at most. We are not aware of any approach that can stage a secure continuous proxy auction, which is both decentralized and privacy preserving concerning the highest bid after the auction closes. Achieving this kind of privacy means that the bid schedule of the highest bidder is never fully resolved in the following protocol. The suggested protocol using asymmetric encryption satisfies correctness in a way that winning bidder and corresponding price are accurately and transparently determined. Accordingly, bids can never be repudiated by any agents and the possibility for successful collusion among malicious auctioneers is extremely low.

Furthermore, the protocol does not require neither any bidder nor most of the auctioneers to remain active throughout the whole auction.

3. REQUIREMENTS

For an auction as indicated above, the following main requirements have been identified. On the one hand, there are four main requirements pertaining to the role of the auctioneers (A1-A4). On the other hand, there are five requirements referring to the bidding process (B1-B5).

- *Second-price (A1):*
  The auctioneers jointly determine the price, which is equal to the second highest bid amount plus an increment.

- *Secret highest bid (A2):*
  No participant – including all auctioneers – but the highest bidder can ever reveal the highest bid.

[1]For a detailed overview of secure auction protocols see [3].

- *Resistant to bidder exclusion (A3):*
  Neither a single auctioneer nor a coalition of auctioneers is able to exclude bidders by illegitimately dropping bids.
- *Robust to paralysis attacks (A4):*
  Neither a single auctioneer nor a coalition of auctioneers is able to block the protocol.
- *Unrestricted bidder access (B1):*
  Any bidder can submit bids without prior registration at any time. This means that a bidder can spontaneously join the auction.
- *Iterative (B2):*
  Bids can be submitted iteratively with the standing highest price revealed as information feedback.
- *Asynchronous (B3):*
  Bidders can independently submit bids at any time during the bidding phase. Only when submitting a bid must a bidder be online. Under no circumstances are all bidders required to be online at a time.
- *Single independent key (B4):*
  For participation, each bidder needs only one single key that is additionally not dependent on any other peer's key.
- *Non-repudiation (B5):*
  The winning bidder cannot deny the submission of the winning bid.

An auction protocol that achieves those requirements is secure in a sense that there is no single point of failure, assured bid submission and protected bid acceptance as well as a high degree of robustness against paralysis attacks. We propose such an auction protocol drawing on asymmetric cryptography.

4. PROTOCOL DESCRIPTION

The auction protocol we present realizes an ascending iterative proxy auction that is complemented by a special secure bidding procedure. Both pieces found the basis for a decentralization of the auction protocol. In essence, we use multiple auctioneers in different groups to prevent one single auctioneer from obtaining complete control over the auction process.

The intuition of the auction protocol is as follows: Our main goal being the protection of the highest bid amount throughout and after the auction (A2), we produce a bid chain of monotonously increasing bidding steps for any bid. We then use the common public key of auctioneer groups for encrypting each bidding step with one such key. Whenever an auctioneer group receives a bid chain, one of the group members decrypts the next encrypted bidding step, if his private group key is applicable and the preceding bidding step in the chain is not higher than the standing highest bid. In case his key is not applicable, he passes the bid chain on to the corresponding auctioneer group. Once a newly decrypted bidding step is higher than the standing highest bid, the respective auctioneer group broadcasts this bidding step to all other auctioneer groups as the new standing highest bid. During the auction process, each auctioneer group holding a partially decrypted bid chain only passes it on to the next auctioneer group in the bid chain, if the bidding step they decrypted is not higher than the standing highest bid. As a consequence of this bid decryption scheme, the bid chain containing the highest standing bid is kept partially encrypted and stays within one auctioneer group, while all other bid chains are fully decrypted.

A detailed description of the auction protocol is given in the following.

4.1 Initial auction setup

At the outset of the auction, seller S has to create a document D describing the auction. This document includes the description of the items for sale and the particular auction procedure including all instance parameters such as ending rule or minimum price. As above-mentioned, this paper is devoted to a single unit ascending proxy auction. The basic concept, however, is certainly not restricted to this special case, as it analogously works for other iterative auction protocols with even multiple units for sale.

Document D will be used to determine the auctioneers and their groups that share the same public/private key pair. In order to ensure authenticity of document D, seller S has to digitally sign D using the private key of his public/private key pair, which is certificated by a trusted party.

The distribution of an auction mechanism onto a number of auctioneers draws on the following group-based approach.

Starting from a desirably larger number A_{total} of auctioneers responsible for the protocol, the number of groups G_{number} and their group size G_{size} can be determined. We use the following calculation:

$$\begin{aligned} G_{size} &= \lfloor log_x(A_{total}) \rfloor \\ G_{number} &= \lfloor \frac{A_{total}}{G_{size}} \rfloor \end{aligned}$$

Accordingly, we use the base x logarithm of the total number of auctioneers A_{total} to determine the size of any auctioneer group G_{size}. It is desirable to choose the total number of auctioneers A_{total} as a power of x such that all auctioneers are assigned to a group. Otherwise, only the integer part will be used. We assume that x is common knowledge throughout the auction. For the number of groups, G_{number}, we divide the total number of auctioneers A_{total} by the group size G_{size} and take the integer part. This approach provides many auctioneer groups relatively small in size.

After having calculated G_{size} and G_{number}, the auctioneers themselves and their membership in groups have to be identified.

This identification must be deterministic and traceable, but hard to anticipate. In particular, the seller himself must not be capable of influencing the selection process. Otherwise, he could select collaborating or malicious nodes in the set of auctioneers.

Hence, we employ the description document D for the selection. One approach is the application of a one-way hash function. Such a function maps arbitrary input onto a result of fixed length. Typical hash functions generate a 128-bit or 160-bit output value. Starting with the hash value of the description document D, a chain of hash values can be calculated for any auctioneer.

$$H_k(D) \quad = \quad \underbrace{H(H(H(\ldots H(D))))}_{k+1 \text{ times}}$$

Given an addressing mechanism, which is capable of mapping such hash values to distinct nodes, a chain of auctioneer nodes can be derived from the chain of hash values.

Such mechanisms are commonly available in structured peer-to-peer networks like CAN [12] or Chord [16]. The configuration of auctioneer addresses in groups are computed by using the following equation, where A_{ij} is the j-th auctioneer in the i-th group.

$$Address(A_{ij}) = H_{i \cdot G_{size}+j}(D) \text{ where } 0 \leq i < G_{number} \text{ and } 0 \leq j < G_{size}$$

Having defined groups, the members of each group have to generate a common group public/private key pair. For simplicity, one auctioneer per group generates a public/private key pair and distributes that key pair to all other auctioneers inside the group using the individual public key of each group member.[2]

After a successful conduct of this auction setup, which includes determination of the number and size of groups G_{number} and G_{size}, selection of group members and group-based key generation, we obtain the following entities:

$$\begin{aligned} G_i &= \text{group } i \text{ of auctioneers, where } 0 \leq i < G_{number} \\ K_i &= \text{public key of group } G_i \\ A_{ij} &= \text{auctioneer } j \text{ of group } i \text{ using public key } K_i, \\ &\quad \text{where } 0 \leq j < G_{size} \end{aligned}$$

4.2 Placing a bid

Having set up the auction, potential buyers can join by placing bids. In our ascending proxy auction, the winning bidder has to pay the price of the second highest bid. As described in section 1, a bidder wants to hide as long as possible his highest bid amount, which may reflect his true valuation.

If a bidder has a valuation v, he offers successively increasing bids up to v.[3] If he wins the auction, his highest bid can be kept secret to anyone else, including the auctioneers. Our procedure makes it possible, but not necessary for the bidder to observe the auction during its whole runtime in order to receive information feedback.

The approach at hand gives the bidder the possibility to place a series of bids and ensure that bids are only revealed if necessary for the auction process. When a bidder joins an auction, he can retrace the number and size of auctioneer groups, G_{number} and G_{size}, by using the same algorithm as the seller. This information can be derived from the auction description document as described in the previous section.

According to his bidding strategy, a bidder will reasonably submit a bid B with a price $p \leq v$. For this purpose, he formulates a bid chain BC of monotonously increasing bidding steps[4] starting from a value $< p$ (e.g. the current maximum bid of the auction) and ranging to p with different increments. Each bidding step in the chain is digitally signed by the bidder to ensure non-repudiation.

The bidder can reproduce A_{ij}, the auctioneer addresses with group-association, applying the same calculations as the seller. From this, he arbitrarily chooses a hopping sequence of auctioneer groups HS (described in the formula below) and receives the respective public keys. The sequence is then used to encrypt the bid chain BC.

$$HS_i \quad = \quad j \quad \text{where } 0 \leq j < G_{number}$$

The bidder starts by encrypting the *highest* bidding step with the first public key K_{HS_0} of the hopping sequence. With the next key of HS, the bidder encrypts the second highest bidding step including the hash value of the highest bidding step and the encrypted highest bidding step. This procedure is repeated until all bidding steps are encrypted. The lowest encrypted bidding step and the hash value of the lowest bidding step are then transmitted to the auctioneer group whose key was used to encrypt the lowest bidding step.

The following formulas illustrate the encryption of the bid chain from the highest to the lowest bidding step. This procedure guarantees that a previous (lower) bidding step must be decrypted correctly before the next (higher) step can be decrypted. In the formulas, E_i denotes the encryption with key K_i, S_L the signing by bidder L, B_i the i-th bid of the bid chain, $H(B_i)$ the hash value of bidding step B_i, and EB_i the i-th encrypted bid of the bid chain BC.

$$\begin{aligned} EB_n &= E_{HS_0}(S_L(B_n)) \\ EB_{n-1} &= E_{HS_1}(S_L(B_{n-1}), S_L(H(B_n)), EB_n) \\ &\cdot \quad \cdot \quad \cdot \\ EB_i &= E_{HS_j}(S_L(B_i), S_L(H(B_{i+1})), EB_{i+1}) \\ &\cdot \quad \cdot \quad \cdot \\ EB_1 &= E_{HS_{n-1}}(S_L(B_1), S_L(H(B_2)), EB_2) \\ EB_0 &= S_L(H(B_1)), EB_1 \end{aligned}$$

Having constructed the encrypted bid chain, the bidder transmits EB_0 to the group of auctioneers which possesses the key $K_{HS_{n-1}}$.

If each bid chain consists of a fixed number n of bidding steps and the bid value p is reached significantly before step n, other bidders or auctioneers are not able to predict the value of p from the starting value and/or other parameters like the increments or number of bidding steps before the bid chain is completely revealed. Accordingly, n has to be chosen sufficiently large.

4.3 Bid evaluation

An auctioneer receiving a bid chain starting with EB_0 will at first verify if his group key K_i and the encryption key of EB_1 do match.

If this check is successful, the receiver will propagate EB_0 to all group members, otherwise convey EB_0 to the applicable group. Subsequently, a subset of all group members (randomly chosen) will decrypt EB_1 to $S_L(B_1)$, $S_L(H(B_2))$ and EB_2. After decryption the member will propagate the signed bidding step $S_L(B_1)$ to all other group members. This procedure enables all group members to verify valid decryption by hashing B_1 and comparing the result to $H(B_1)$ included in EB_0. If those do not match, another auction-

[2]Another possibility, not addressed in this paper, is the generation of a distributed public/private key pair described in [2].

[3]For simplicity we presume the Independent Private Value Model.

[4]Note that *strict monotony* is not required.

eer of the respective group has to repeat this process until validity is established.

Having successfully checked validity of the decrypted bidding step B_1, and B_1 beating the standing highest bid, the auctioneer group will create a bid confirmation for B_1 and send this confirmation back to the bidder L. The auctioneer group will broadcast the amount of B_1 as the standing highest bid and the hash value $H(S_L(B_1))$ as corresponding bid of to all auctioneers. If bid B_1 does not beat the leading bid, the group (some randomly selected members) will transfer $S_L(B_1)$, $S_L(H(B_2))$ and EB_2 to the next auctioneer group, depending on the key hopping sequence chosen by bidder L. Any following auctioneer group in the hopping sequence will repeat the previous steps until either the end of the bid chain is reached or the auction terminates. Hence, upon termination, all bid chains – except for the winning bidder's – end up fully decrypted.

A premature decryption of a bidding step EB_i can be prevented, since each auctioneer group can check whether the standing highest bid comes from the same bidder L by comparing the value of $H(S_L(B_{i-1}))$ and the published hash value of the standing highest bid. If the hash values match, one or more auctioneers in the previous auctioneer group could be malicious, as they incorrectly passed the bid chain to the next auctioneer group. Also, if an auctioneer receives multiple different hash values from different auctioneers of the previous group, this suggests that there are malicious auctioneers among the previous group.

4.4 Security and threat analysis

Most of the security requirements for auctioneers (see section 3) can be fulfilled by applying the presented group-based approach. While each auction is governed by a set of auctioneers instead of a single one, the auctioneers themselves are separated into different groups where each group is only responsible for one step of the auction process. As long as there is at least one valid auctioneer in each auctioneer group, our bid chaining protocol works correctly.

Second-price (A1): At the end of the auction, all bid chains, except the one of the winning bidder, have been completely revealed. This means that the second-highest bid chain is fully revealed, determining the price for the winning bidder.

Secret highest bid (A2): An auctioneer group in possession of the leading bidder's bid chain will convey the next bidding step EB_{i+1} to the specified group only if a better standing highest bid is announced. Only then can EB_{i+1} be decrypted. To illegitimately obtain the highest bidding step of the winning bidder with certainty, an attacker would have to compromise all auctioneer groups in the key hopping sequence of the bidder. However, this hopping sequence is unknown to the attacker.

Resistant to bidder exclusion (A3): Permanently rejecting bids is only possible, if every auctioneer is compromised by the attacker. Otherwise, another (obedient) auctioneer accepts the bid and introduces it into the auction process.

Robust to paralysis attacks (A4): As every group consists of two or more members that are all redundant to each other, it is guaranteed that blocking the auction protocol by not decrypting or not passing on bid chains is impossible unless the attacker controls a majority of all auctioneers of an auction.
More precisely, to block the auction protocol all members of an auctioneer group have to be compromised. Even one obedient auctioneer facing an otherwise malicious group will ensure that bids encrypted with his group key will be processed properly. Taking over one auctioneer group completely will only block some arbitrary bids, but not the whole auction. To block a specific bidder's bid, the attacker must know the respective hopping sequence, which is private knowledge of the bidder. Since every bid has its own key hopping sequence, an attacker must overtake at least one auctioneer group out of each (unknown!) hopping sequence to block a specific bidder or even the whole auction, respectively. Consequently, our approach is highly immune against minority paralysis attacks, but still relies on a minimum of obedient auctioneers.

Unrestricted bidder access (B1): The initial auction setup only involves the auctioneers. Any bidder can retrace the auctioneer addresses and groups as well as retrieve their public keys on demand. Likewise, the winner and price determination are performed by the auctioneers.

Iterative (B2): Inherent to the iterative nature of the proposed auction protocol this requirement is fulfilled.

Asynchronous (B3): Each bidder can submit a bid at any time (during the auction's bidding stage); he only has to be online for the short time necessary for submission of his own bid.

Single independent key (B4): Key management is simple for bidders participating in an auction. A bidder just needs a public/private key pair (usable for digital signatures), which can even be used for several auctions.

Non-repudiation (B5): As each bidding step is only accepted with a valid digital signature, the winner cannot deny that he submitted his signed winning bid.

5. CONCLUSION

We present a secure mechanism for distributed ascending proxy auctions. The proposed approach draws on standard cryptographic mechanisms. Thus, any one-way hash function and any asymmetric encryption algorithm is applicable for implementation.

The approach eliminates the dependency on one single auctioneer. Additionally, the winning bidder can hide his true valuation, respectively his highest bid. Using an encrypted bid chain for bidding allows that only a limited amount of information is revealed to each auctioneer. Any bidder can freely decide which selection of auctioneer groups to trust. Robustness is achieved by forming groups of auctioneers, where only one group member suffices to decrypt a bidding step – the other group members can verify the decryption.

In contrast to previous distributed second-price auction mechanisms, our approach is suitable for iterative open-cry auctions. It is never necessary for all participants to be online at the same time. All a bidder needs to do is to convey his bid chains; no further activity is required on his side. The involved auctioneer groups must be accessible during the whole process, but a single obedient group member being online at a time is sufficient to conduct the auction process with a minimal standard of security.

As a next step, an implementation of the proposed mechanism is planned. In the SESAM project at the University of Karlsruhe [6], a prototype of a P2P auction system has already been realized, which will be enhanced by the secure ascending proxy auction protocol.

6. REFERENCES

[1] O. Baudron and J. Stern. Non-interactive private auctions. In *5th Annual Conference on Financial Cryptography*, pages 300–313, 2001.

[2] D. Boneh and M. Franklin. Efficient generation of shared RSA keys. *Lecture Notes in Computer Science*, 1294:425+, 1997.

[3] F. Brandt. A verifiable, bidder-resolved auction protocol. In R. Falcone, S. Barber, L. Korba, and M. Singh, editors, *Proceedings of the 5th AAMAS Workshop on Deception, Fraud and Trust in Agent Societies (Special Track on Privacy and Protection with Multi-Agent Systems)*, pages 18–25, 2002.

[4] F. Brandt. Fully private auctions in a constant number of rounds. In R. N. Wright, editor, *7th Annual Conference on Financial Cryptography (FC)*, Lecture Notes in Computer Science (LNCS), pages 223–238, 2003.

[5] C. Cachin. Efficient private bidding and auctions with an oblivious third party. In *6th ACM Conference on Computer and Communications Security*, pages 120–127, 1999.

[6] M. Conrad, J. Dinger, H. Hartenstein, M. Schöller, and M. Zitterbart. Combining service-orientation and peer-to-peer networks. In *Kommunikation in verteilten Systemen (KiVS)*, pages 181–184, 2005.

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

[8] H. Kikuchi. Resolving winner and winning bid without revealing privacy of bids. In *Proceedings of the International Workshop on Next Generation Internet (NGITA)*, pages 307–312, 2000.

[9] H. Kikuchi. (m+1)st-price auction protocol. In *FC '01: Proceedings of the 5th International Conference on Financial Cryptography*, pages 351–363, London, UK, 2002. Springer-Verlag.

[10] H. Kikuchi, M. Hakavy, and J. Tygar. Multi-round anonymous auction protocols. *TIEICE: IEICE Transactions on Communications/Electronics/Information and Systems*, 1999.

[11] D. Lucking-Reiley. Vickrey auctions in practice: From nineteenth-century philately to twenty-first-century e-commerce. *Journal of Economic Perspectives*, 14(3):183–192, 2000.

[12] S. Ratnasamy, P. Francis, M. Handley, R. Karp, and S. Shenker. A scalable content-addressable network. In *ACM SIGCOMM Conference*, pages 161–172, San Diego, 2001. ACM Press.

[13] M. S. Robinson. Collusion and the choice of auction. *RAND Journal of Economics*, 16(1):141–145.

[14] M. H. Rothkopf, T. J. Teisberg, and E. P. Kahn. Why are vickrey auctions rare? *Journal of Political Economy*, 98(1):94–109, 1990.

[15] K. Sakurai and S. Miyazaki. An anonymous electronic bidding protocol based on a new convertible group signature scheme. In *ACISP '00: Proceedings of the 5th Australasian Conference on Information Security and Privacy*, pages 385–399, London, UK, 2000. Springer-Verlag.

[16] I. Stoica, R. Morris, D. Karger, M. F. Kaashoek, and H. Balakrishnan. Chord: A scalable peer-to-peer lookup service for internet applications. In *SIGCOMM01*, San Diego, California, USA, 2001.