A trustworthy Internet auction model with verifiable fairness

Gen-Yih Liao and Jing-Jang Hwang

The authors

Gen-Yih Liao is a PhD student, and **Jing-Jang Hwang** is a Professor, both at the Institute of Information Management, National Chiao Tung University, Hsinchu, Taiwan.

Keywords

Internet, Auctions, Computer privacy, Electronic commerce

Abstract

Describes a novel Internet auction model achieving verifiable fairness, a requirement aimed at enhancing the trust of bidders in auctioneers. Distrust in remote auctioneers prevents bidders from participating in Internet auctioning. According to proposed survey reports, this study presents four characteristics that render the Internet untrustworthy for bidders. These intrinsic properties suggest that auction sites not only follow auction policies, but provide customers with evidence validating that the policies are applied fairly. Evidence of verifiable fairness provides bidders with a basis for confidence in Internet auctions. Cryptographic techniques are also applied herein to establish a novel auction model with evidence to manifest and verify every step of the auctioneer. Analysis results demonstrate that the proposed model satisfies various requirements regarding fairness and privacy. Moreover, in the proposed model, the losing bids remain sealed.

Electronic access

The research register for this journal is available at
http://www.mcbup.com/research_registers

The current issue and full text archive of this journal is available at
http://www.emerald-library.com/ft

Internet Research: Electronic Networking Applications and Policy
Volume 11 · Number 2 · 2001 · pp. 159–166
 · ISSN 1066-2243

Introduction

The rapidly developing Internet provides an attractive environment for on-line auctions, because the Internet crosses national borders so as to expand the scope of potential dealers. Besides, the facilitated bidding process in a paperless environment reduces a significant amount of cost. Internet auctions, therefore, have become promising examples of B-to-C electronic commerce. Yahoo!Auction (http://auctions.yahoo.com/) and eBay (http://www.ebay.com) are two successful examples.

Despite the successes, auction sites are still facing challenges arising from the intrinsic properties of the Internet. Since the net is a black box to bidders, they cannot verify the remote processes run by the auctioneer as they can in a traditional auction. Moreover, they worry about the leaking of personal information (e.g. bid values) by the auctioneer to the bidders' competitors who could unfairly take advantage. These concerns lead to distrust that prevents some Internet users from participating in Internet auctions.

Increased trust demands an auction model with verifiable fairness, in which bidders can verify with evidence whether fairness is maintained. Current literature has addressed satisfying fairness based on various trust assumptions. A common approach is to trust the auctioneer (Franklin and Reiter, 1995, 1996; Kikuchi *et al.*, 1999; Kudo, 1998; Sako, 2000). Some works rely on secret sharing concepts (Shamir, 1979) to distribute the trust among several servers to avoid the need for total trust (Franklin and Reiter, 1995; 1996; Kikuchi *et al.*, 1999; Sako, 2000). Other work endeavors separation of duties (Kudo, 1998). Besides, Naor *et al.* (1999) proposed a privacy preserving scheme while presuming no conspiracy between a seller and the auctioneer. These assumptions might not convince a foreign user of the Internet, as he obtains no proof of how those servers work. None of the work aiming at verifiability (Kudo, 1998; Naor *et al.*, 1999; Sako, 2000) offers

The authors wish to thank anonymous reviewers for their valuable suggestions. This research was supported by grant NSC 89-2213-E-009-017 from The National Science Council, Taiwan.

Internet Research: Electronic Networking Applications and Policy
Volume 11 · Number 2 · 2001 · 159–166

sufficient evidence to verify all requirements related to fairness.

This work discusses the trustworthiness of an Internet auction model from a technical point of view. That is, the study focuses on technical solutions while excluding organizational and marketing discussion. The following two sections examine the intrinsic properties of the Internet to establish a technically sound environment and propose a complete set of requirements for Internet auctions.

Intrinsic characteristics of the Internet

Open connectivity
The Internet is a public medium so all bid transmissions are exposed to attacks in the middle, including various forms of eavesdropping and tampering.

Opacity
The Internet is a black box. Bidders can hardly verify whether an auctioneer fairly follows its policies as in a traditional auction. For example, an auctioneer might leak bid information to a bidder's competitors, who therefore have an unfair advantage in forthcoming auctions. In addition to privacy infringement, an auctioneer might also infringe the fairness principle by failing to return goods or receipts, which problem is a major issue for auction sites (NACAA/CFA, 1999).

These concerns over auctioneers have been illustrated. In a fraud research survey, CyberSource ranks "lack of confidence by consumers" the number one concern of virtual businesses (see CyberSource Corp., 1999). Although opacity is an inherent property of the Internet, auction sites must alleviate relevant concerns to attract more bidders.

Lack of a trustworthy payment instrument
Despite much research focusing on electronic payment over the Internet, current payment instruments have not been met with much confidence according to several survey reports.

In the fraud research by CyberSource, 28 per cent of the respondents reported experiencing frauds involving stolen credit cards, which crime is the most prevalent. The *Eighth Annual NACAA/CFA Consumer Complaint Survey Report* (1999) also expresses the same phenomenon. Still other reports present similar concerns of customers over using credit cards via the net (Baker, 1999; Furnell and Karweni, 1999).

Weak binding of identities
Associating a virtual identity in the Internet with an entity in the physical world is extremely difficult. In Yahoo!Auction, for instance, a bidder is linked to the auction site through an e-mail account that can be easily abandoned. Lack of traceability facilitates cheating like submitting phantom bids and shilling. However, before governments agree to a common identification structure in the Internet, law differences among countries form obstacles of binding identities.

Requirements for Internet auction

The proposed requirements do not address payment issues due to the lack of any trustworthy payment instrument. The auctioneer in the proposed model plays the role as a broker between bidders and a seller. Moreover, the open connectivity of the Internet strongly requires an auction model which provides rigid protection during transmission. Fairness is compromised when bids are eavesdropped before the submission deadline.

This study proposes the notion of verifiable fairness to avoid the weaknesses brought about by opacity. Fairness is defined as a state satisfying a collection of auction policies under which a bidder gains no advantage over others. If a bidder holds evidence that the auction policies are correctly followed, verifiable fairness is satisfied. The following properties concerning fairness are required for sealed-bid auction in the Internet:

- Property 1. *Privacy before bidding*: a bidder cannot know the bids of others before bidding.
- Property 2. *Deadline enforcement*: the submission deadline is strictly regulated so that no one can bid when bid submission ends.
- Property 3. *Bid integrity*: during transmission and processing of bids, no bid will be extracted or tampered.

Internet Research: Electronic Networking Applications and Policy
Volume 11 · Number 2 · 2001 · 159–166

- Property 4. *Validity*: the winner bids highest among all correct bids.
- Property 5. *Non-repudiation*: the winner cannot repudiate his bid.

Note that a different definition of a winner is adopted due to weak binding of identities. Because a fraudulent bidder might deliberately quit his registration after cheating, the winner might be the one who has submitted a smaller bid. Nevertheless, the winner must bid higher than any other correct bid and may not repudiate his bid.

As well as maintaining privacy before the end of bid submission, preserving privacy after the opening of bids is essential for on-line auction. The range of bid values can be derived from past bidding records on similar objects. Therefore, a bid should be kept confidential unless it is the winning one. This leads to Property 6.

- Property 6. *Privacy of losing bids*: no one, including the auctioneer, can learn the content of losing bids.

Preliminaries

Cryptography is the subject of secure transmission. A sender encrypts a plaintext with an encryption key and transmits the ciphertext to prevent messages from being observed. Only recipients with the correct decryption key can decrypt the ciphertext.

The encryption key may differ from the decryption key. Public key cryptography involves a pair of keys: a private key and a public key. The private key is used for signing digital signatures and decrypting messages, while the public key is used for verifying signatures and encrypting messages. Therefore, public keys may be published for convenient access. Recent literature has proposed several public key algorithms that guarantee the difficulty of deriving a private key from its corresponding public key using up-to-date computer technology. RSA (Rivest *et al.*, 1978) and ElGamal (ElGamal, 1985) are two well-known examples of public key algorithms.

A third party called the Certificate Authority (CA) issues public key certificates to manifest the validity of public keys. Such certificates, which can be used to verify the identities of key owners, facilitate identifying virtual entities in future cyberspace.

Placing a secret under the control of only one entity is occasionally unsafe, especially when confidence towards the secret holder is not sufficient. Secret sharing schemes solve this problem by splitting a secret into n pieces. At least k pieces are required to uncover the secret; k-1 or fewer pieces construct no secret. k is called the threshold of a secret sharing scheme (Shamir, 1979).

A hash function accepts a variable-length input and produces a fix-length output. A cryptographic hash function is characterized by one-wayness. That is, inferring the input from the output of a cryptographic function is extremely difficult. Two examples that are recognized as secure against attacks are SHA-1 (NIST, 1995) and RIPEMD-160 (Dobbertin *et al.*, 1996).

Although it is difficult for Internet users to verify each other's identities, a technique called "challenge and response" may resolve the problem of authentication. Both the verifier and the proof-provider agree to a secret number S in advance. During verification, the verifier randomly chooses a number r and sends it to the proof-provider, who then computes a predetermined function of the secret number S and the random number r. The function value is transmitted back to the verifier. The function value enables the verifier to determine the proof-provider is authentic.

"Cut-and-choose" is another technique to verify that data conform to some claimed property without compromising privacy of the data. The proof-provider can encrypt many sets of data and send them to the verifier. Next, the verifier randomly selects some of the encrypted sets and asks the proof-provider to decrypt the chosen sets. If the decrypted sets of data possess the claimed property, the unselected sets have a high probability of owning the claimed property but remain confidential, as the verifier cannot decrypt without the decryption key.

In the following, $PK_{user}(message)$ denotes a ciphertext generated by encrypting a message with the public key of a user. A digital signature is denoted by $SK_{user}(message)$, indicating that a

Internet Research: Electronic Networking Applications and Policy
Volume 11 · Number 2 · 2001 · 159–166

message is signed by a user's private key. Users are denoted by their initials. For example, the auctioneer is denoted by "A" and his signature on a message is referred as $SK_A(message)$.

Literature review

Several works employ the secret sharing concept to divide bids into n auction servers (Franklin and Reiter, 1995; 1996; Kikuchi *et al.*, 1999; Sako, 2000). Bidders in these solutions must completely accept the threshold assumption but cannot verify fairness with evidence. In Sako's work (2000), for example, privacy of losing bids is preserved because the decryption functions of these bids are shared among n servers. Protection of losing bids requires at least k correct servers under the threshold assumption, which bidders are unable to verify.

Nurmi proposed a different approach in that an auctioneer can only accept encrypted bids but has no right to compare bids; rather, bidders compare their bids and determine a winner among themselves (Nurmi, 1994). This approach might maintain privacy of losing bids, as no one including the auctioneer can learn the content of bids. Unfortunately, if a bidder cheats by claiming himself the winner, other bidders cannot verify this result. Therefore, Nurmi's approach does not ensure validity, which also leads to fairness infringement.

In Kudo's method, functions of an auctioneer are realized in three service providers. An auction service provider is responsible for determining the winning bid among encrypted bids. The decryption key is under the control of a key service provider, which is assumed never to leak the key until the time when the service provider certifies that the deadline has passed (Kudo, 1998). This premise hardly convinces remote bidders who distrust an auctioneer, even when its functions are dispersed into several parties.

In the verifiable auction model proposed by Naor *et al.* (1999), a seller sends an auctioning program to the auctioneer through a cut-and-choose procedure. This program accepts encrypted bid prices from bidders and generates the winner and the winning price. The encryption achieves privacy and verifiability because all can validate the result with the program that may be released after auctioning. However, if a seller conspires with the auctioneer, the content of bids will be disclosed.

Briefly, current solutions assume the trustworthiness of an auctioneer by secret sharing, separation of duties, or no collusion. In other words, violating these assumptions enables an auctioneer to corrupt the auction. This paper proposes an auction model in which bidders can verify every step of an auction with evidence published by the auctioneer and sellers. Our solution satisfies Property 6, since bidders can absolutely control information to recover bids even after bids are submitted.

The proposed auction model

Step 1. Registration

Bidders and sellers send their digital certificates to the auctioneer. After validation through a challenge and response procedure, the auctioneer publishes all the certificates including his own. The identity information in the certificates will be used to identify a participant in later phases.

For bidders to commit to their secret bids, the auctioneer announces a cryptographic hash function $h()$. In addition, an auction number *aid* is also declared to differentiate various auctions.

Step 2. Preparing bids

This protocol represents a bid value bv as the difference of two integers, a_1 and a_2 ($bv = a_2 - a_1$). The link between a_1 and a_2 must not be derived to protect confidentiality of bid values. Therefore, a bidder b generates his bid by creating two *half-bids* in the form of two pairs, $(PK_s(a_1), r_1, 1)$ and $(PK_s(a_2), r_2, 2)$. The first items in both half-bids are enciphered with the public key of the seller. For a random number r, $r_1||r_2 = h(r||SK_b(aid||ID_b||bv))$, where r is chosen by bidder b and $||$ means concatenation.

Step 3. Submitting the bids

While submitting a bid, a bidder must separately send the two half-bids to the auctioneer instead of casting the total bid. The separate submission

Internet Research: Electronic Networking Applications and Policy
Volume 11 · Number 2 · 2001 · 159–166

prevents the auctioneer from deriving original connections among half-bids. The auctioneer must return a signed receipt as proof of half-bid transmission. A bidder must therefore retain two receipts to prove his bidding.

Evidence 1: two receipts signed by the auctioneer in the form of $SK_a(PK_s(a_{ij}), r_{ij}, j)$.

When bid submission ends, the auctioneer receives a set of triples $(PK_s(a_{ij}), r_{ij}, j), j\varepsilon\{1,2\}$, $1 \leq i \leq n$, where n indicates the number of bidders. a_{i1} and a_{i2} are the two integers chosen by the i-th bidder. The auctioneer then publishes a signed list of $r_{i1}||r_{j2}, 1 \leq i,j \leq n$. Bidders can verify their bid if their own $r_1||r_2$ is contained in the list; otherwise Evidence 1 attests to the fault of the auctioneer.

Evidence 2: a list of $r_{i1}||r_{j2}$, published by the auctioneer.

After publishing the check value, the auctioneer transfers the set of triples to the seller.

Step 4. Opening the bids

After receiving the half-bids from the auctioneer, the seller verifies the received set with Evidence 2. If the verification succeeds, the seller decrypts the encrypted $PK_s(a_{ij})$ in all the half-bids and matches each of first-half-bids (i.e. $(a_{i1}, r_{i1}, 1)$) with each of second-half-bids (i.e. $(a_{j2}, r_{j2}, 2)$). This matching generates a list of pairs $(r_i1||r_{j2}, a_{j2} - a_{i1}), 1 \leq i,j \leq n$.

Evidence 3: a list of pairs $(r_{i1}||r_{j2}, a_{j2} - a_{i1})$ signed by the seller.

The seller then sorts the list by $a_{j2} - a_{i1}$ and releases the whole list. To ensure that the seller does not alter or extract any pair in the list, bidders can compare Evidence 3 with Evidence 2. Bidders must validate whether their own $r_1||r_2$ is associated with the correct bid (i.e. $a_{j2} - a_{i1}$) in the list.

Step 5. Determining the winner

The seller announces n^2 deadlines of identifying bidders to determine the winner. In the k-th time slot, a bidder who is ranked in the k-th place offers to the auctioneer his random number r as well as the signature signed on the auction number, his bidder *ID*, and the bid value (i.e. $SK_b(aid||ID_b||bv)$). Since not all n^2 values are real bids, the bidder who first identifies himself is determined as the winner, if the following conditions are met:

(1) The auctioneer verifies the signature with the certificate of the bidder.
(2) The auctioneer verifies if $r_1||r_2 = h(r||SK_b(aid||ID_b||bv))$.

After successful verification, the auctioneer signs on $SK_b(aid||ID_b||bv)$ as well as the random number r before publishing. All the other bidders and the seller can now conduct the same checks to validate the winner.

Evidence 4: $SK_a(SK_b(aid||ID_b||bv))$ and $SK_a(r)$, the auctioneer's signatures on a bid.

A simple example

Alice, Bob, and Carol are three bidders participating in an auction. Their bid values are 50, 70, and 45 respectively. After creating their half-bids with three pairs (20, 70), (50, 120), and (15, 60), all of the bidders submit the half-bids to the auctioneer and receive the corresponding Evidence 1. Figure 1 illustrates Alice's bidding. Notably, Alice sends the two half-bids at a random interval or from different Internet addresses to prevent the auctioneer from learning the relationship between her half-bids.

Alice's Evidence 1: $SK_a(PK_s(70), r_2, 2)$ and $SK_a(PK_s(20), r_1, 1)$.

Assume that Carol deliberately interferes with the auction and casts only one half-bid. The auctioneer then obtains five half-bids when the submission ends, as Figure 2 shows. He then publishes his signature on the list of five half-bids as Evidence 2 and then transmits the list to the seller.

Evidence 2: a list $(r_{a1}||r_{a2}, r_{a1}||r_{b2}, r_{b1}||r_{a2}, r_{b1}||r_{b2}, r_{c1}||r_{a2}, r_{c1}||r_{b2})$ signed by the auctioneer.

The seller verifies the received list with the published Evidence 2. If the list is verified, the seller generates a new list by matching each of the first-half-bids with each of the second-half-bids. The list illustrated in Figure 3 is published with the seller's signature as Evidence 3.

Evidence 3: a list of $((r_{c1}||r_{b2}, 105), (r_{a1}||r_{b2}, 100), (r_{b1}||r_{b2}, 70), (r_{c1}||r_{a2}, 55), (r_{a1}||r_{a2}, 50), (r_{b1}||r_{a2}, 20))$ signed by the seller.

Internet Research: Electronic Networking Applications and Policy
Volume 11 · Number 2 · 2001 · 159–166

Figure 1 Alice's bidding

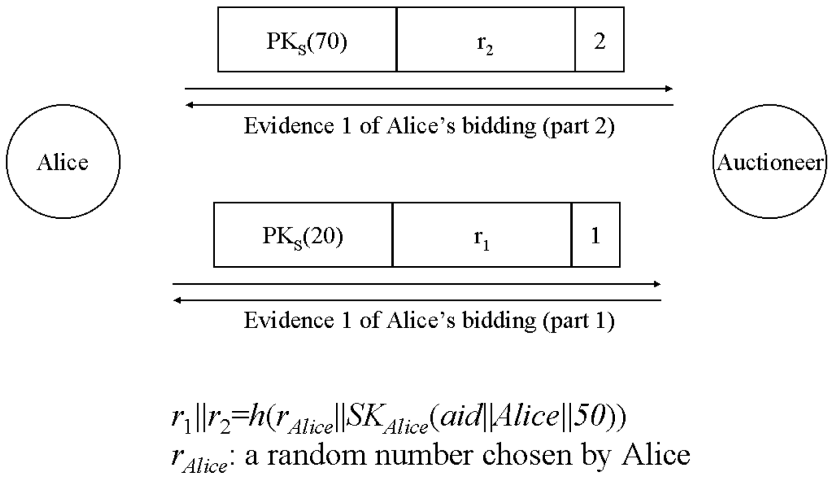
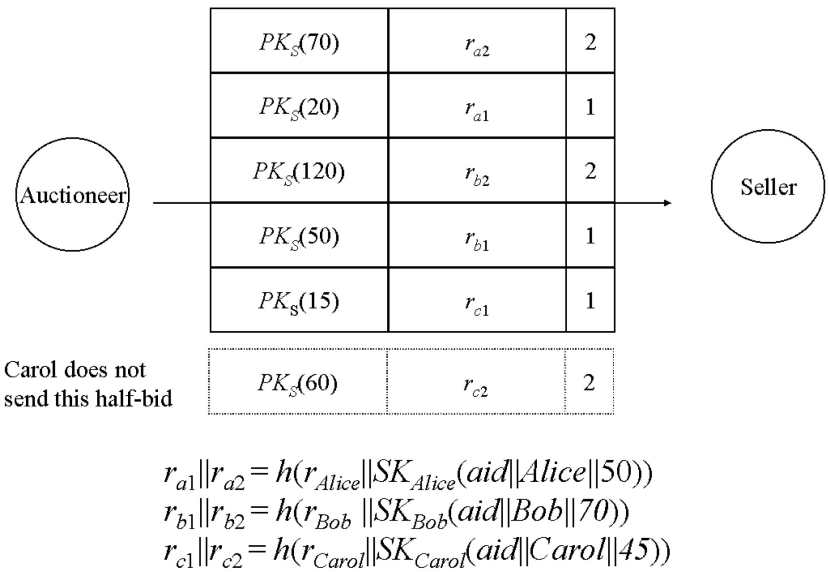


Figure 2 The auctioneer receives all of the half-bids before transferring the bids to the seller



In determining the winner, the seller announces six deadlines. According to the one-wayness property of cryptographic hash functions, it is infeasible to find a random number r' and a signature S' such that $h(r'||S')$ is equal to either $r_{c1}||r_{b2}$ or $r_{a1}||r_{b2}$. Hence, no one can declare himself as the winner by the second deadline. By the third deadline, Bob can offer his random number r_{Bob} and the corresponding signature $SK_{Bob}(aid||Bob||70)$ to win in the auction. Through verification, the auctioneer publishes its signature $SK_a(SK_{Bob}(aid||Bob||70))$ and $SK_a(r_{Bob})$ to prove that Bob is the winner.

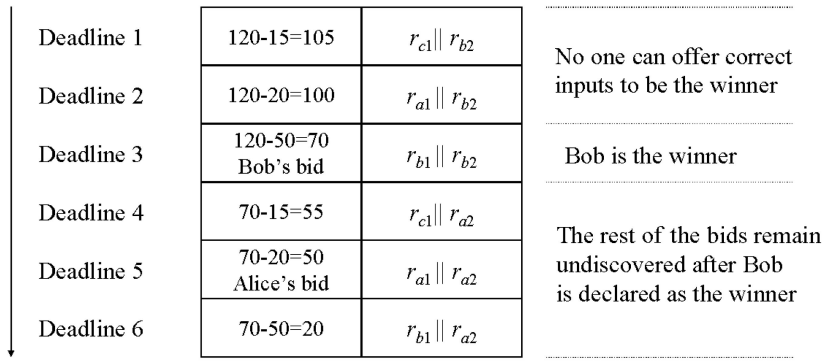
Evidence 4: $SK_a(SK_{Bob}(aid||Bob||70))$ and $SK_a(r_{Bob})$, the auctioneer's signature on the winner's bid.

Discussion

This section first investigates the underlying assumptions of the proposed auction model. The model is then analyzed according to the proposed requirements.

The auctioneer is essentially assumed to control the deadlines. That is, the auctioneer accepts all the bids arriving by the submission

Figure 3 The seller announces the list to determine the winner



deadline and rejects those coming late. Furthermore, the auctioneer is presumed never to fail a bidder who submits a bid or identifies himself as the winner. This assumption is practical because the auctioneer can neither discover the relationships among half-bids nor favor a bidder by eliminating the half-bids of other bidders.

Bidders are assumed to verify Evidence 2 through to Evidence 4. The verification can be automated with a software program. Notably, the proposed model neither assumes that no conspiracy exists between the seller and the auctioneer, nor requires an authority that never leaks a decryption key.

Property 1. Privacy before bidding
The association between two half-bids must be revealed to learn the content of bids. Since only the creator of a bid can know the random number r and sign on $aid||ID_b||bv$, others cannot learn the associations of half-bids only to break the one-wayness property of cryptographic hash functions. Even if an attacker could learn the associations, bid values remain protected as the integers in the two half-bids are encrypted with the seller's public key. In Figure 1, for example, Alice's two integers (e.g. 70 and 20) are encrypted with the seller's public key. Separately submitting two half-bids renders her bid value difficult to derive.

Property 2. Deadline enforcement
Since the auctioneer is assumed to follow the deadlines, no one can bid after the bid submission ends. Moreover, the seller cannot add faked bids as one can verify Evidence 3 with Evidence 2. Therefore, this property is verifiable.

In the example, the auctioneer publishes a list $(r_{a1}||r_{a2}, r_{a1}||r_{b2}, r_{b1}||r_{a2}, r_{b1}||r_{b2}, r_{c1}||r_{a2}, r_{c1}||r_{b2})$ as Evidence 2. Evidence 3, when announced by the seller, should consist of exactly the same elements as Evidence 2. Therefore, false bids inserted by a malicious seller can be detected.

Property 3. Bid integrity
Evidence 1 provides bidders with strong proof that their bids remain intact when they arrive at the auctioneer. Comparing Evidence 1 with the lists published in Evidence 2 and Evidence 3 enables bidders to validate the bidding processes with respect to the auctioneer and the seller.

For example, if Alice obtains a receipt $SK_a(PK_s(20), r_{a1}, 1)$ from the auctioneer, she can be assured that her first-half-bid is not manipulated by attackers during transmission. If Evidence 3 published by the seller does not include $r_{a1}||r_{a2}$, Alice can offer to the auctioneer her Evidence 1 which testifies to the mistake in the seller's operation.

Property 4. Validity.
Every bidder can verify the result with Evidence 4. If a bidder bids higher than the winner, he must have quit during the determination of the winner. Since the auctioneer correctly followed the deadlines, the bids cast by those who quit are considered incorrect and the winner's bid remains the highest from all correct bids.

Internet Research: Electronic Networking Applications and Policy
Volume 11 · Number 2 · 2001 · 159–166

In our example, when the auctioneer declares Bob as the winner, Alice can verify that the signatures in Evidence 4 are valid and that the hash value of $r_{Bob}||SK_{Bob}(aid||Bob||70)$ equals $r_{b1}||r_{b2}$. Succeeding in both checks confirms that Bob bids higher than Alice.

Property 5. Non-repudiation.
Evidence 4 $SK_a(SK_b(aid||ID_b||bv))$ provides strong proof of the identity of the winner. Neither bidder b nor the auctioneer can deny the fact that bidder b wins. In the example, since $SK_a(SK_{Bob}(aid||Bob||70))$ is signed by Bob and by the auctioneer, neither can deny that Bob wins the auction with the winning price of 70.

Property 6. Privacy of losing bids.
Since a losing bidder may keep private his random number r and his signature on $aid||ID_b||bv$, his bid remains undisclosed after the auction. In the example, no one can distinguish Alice's bid among the remaining bids because it is difficult to guess a correct random number r' and produce a signature S' such that $h(r'||S')$ equals $r_{a1}||r_{a2}$.

Conclusion

This paper investigates the current environment of Internet auction and proposes feasible requirements. A new auction model is proposed to satisfy these requirements. The proposed model offers unique features: bidders can verify the auctioning process with evidence, while the privacy of losing bids is arbitrarily preserved.

Management control and brand image are also important in enhancing the trustworthiness of auction sites. Nevertheless, the proposed model emphasizes that verifiable fairness is indispensable to the auction environment. Future research will elaborate on an auction model that can determine a winner who submits the highest bid among all bids (not just correct bids) without sacrificing any of the other requirements.

References

Baker, C.R. (1999), "An analysis of fraud on the Internet", *Internet Research: Electronic Networking Applications and Policy*, Vol. 9 No. 5, pp. 348-59.

CyberSource Corp. (1999), *CyberSource Fraud Research*, www.cybersource.com/fraud_survey

Dobbertin, H., Bosselaers, A. and Preneel, B. (1996), "RIPEMD-160: a strengthened version of RIPEMD", in Gollmann, D. (Ed.), *Proceedings of the 3rd International Workshop on Fast Software Encryption*, Springer-Verlag, Cambridge, pp. 71-82.

ElGamal, T. (1985), "A public key cryptosystem and a signature scheme based on discrete logarithms", *IEEE Transactions on Information Theory*, Vol. 31, July, pp. 469-472.

Franklin, M.K. and Reiter, M.K. (1995), "The design and implementation of a secure auction service", in Meadows, C. and McHugh, J. (Eds), *Proceedings of IEEE Symposium on Security and Privacy*, IEEE Computer Society Press, Oakland, CA, pp. 2-14.

Franklin, M.K. and Reiter, M.K. (1996), "The design and implementation of a secure auction service", *IEEE Transactions on Software Engineering*, Vol. 22, May, pp. 302-12.

Furnell, S.M. and Karweni, T. (1999), "Security implications of electronic commerce: a survey of consumers and businesses", *Internet Research: Electronic Networking Applications and Policy*, Vol. 9 No. 5, pp. 372-82.

Kikuchi, H., Hakavy, M. and Tygar, D. (1999), "Multi-round anonymous auction protocols", *IEICE Transactions on Information & System*, Vol. E82-D, April, pp. 769-77.

Kudo, M. (1998), "Secure electronic sealed-bid auction protocol with public key cryptography", *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences*, Vol. E81-A, January, pp. 20-27.

Naor, M., Pinkas, B. and Sumner, R. (1999), "Privacy preserving auctions and mechanism design", in *Proceedings of the 1st ACM Conference on Electronic Commerce*, ACM Press, Denver, CO, pp. 129-39.

National Association of Consumer Agency Administrators and Consumer Federation of America (1999), *8th Annual NACAA/CFA Consumer Complaint Survey Report*, www.nacaanet.org/survey99.htm

National Institute of Standards and Technology (1995), *Secure Hash Standard*, NIST FIPS PUB 180-1, US National Institute of Standards and Technology, Gaithersburg, MD.

Nurmi, H. (1994), "Cryptographic protocols for auctions and bargaining", in Karhumaki, J., Maurer, H. and Rozenberg, G. (Eds), *Proceedings of Results and Trends in Theoretical Computer Science*, Springer-Verlag, Berlin, pp. 317-24.

Rivest, R.L., Shamir A. and Adleman, L.M. (1978), "A method for obtaining digital signatures and public key cryptosystems", *Communications of the ACM*, Vol. 21, February, pp. 120-26.

Sako, K. (2000), "An auction protocol which hides bids of losers", in Imai, H. and Zheng, Y. (Eds), *Proceedings of the 3rd International Workshop on Practice and Theory in Public Key Cryptosystems*, Springer-Verlag, Melbourne, pp. 422-32.

Shamir, A. (1979), "How to share a secret", *Communications of the ACM*, Vol. 22, November, pp. 612-13.