Adding timestamps to the secure electronic auction protocol *

Min-Shiang Hwang † Eric Jui-Lin Lu† Iuon-Chang Lin ‡

Department of Information Management †
Chaoyang University of Technology
168, Gifeng E. Rd., Wufeng,
Taichung County, TAIWAN 413, R.O.C.
Email: {mshwang,jlu}@cyut.edu.tw
Fax: 886-4-3742337

Department of Computer Science and ‡
Information Engineering,
National Chung Cheng University,
Chaiyi, Taiwan, R. O. C.
Email: iclin@cs.ccu.edu.tw

July 13, 2001

*This research was partially supported by the National Science Council, Taiwan, R.O.C., under contract no.: NSC89-2213-E-324-053.

Adding timestamps to the secure electronic auction protocol

Abstract

Recently, Subramanian proposed a secure electronic auction protocol. It was claim ed that the auction protocol ensured: anonymity, security, privacy, atomicity, and low overhead. However, the sensitive information of payment, such as credit card number, can be revealed by the auctioneer. The bid can be forged by a malicious auctioneer. Also, the situation of two or more bidders offered the same price was not resolved efficiently. In this article, we will improve the robustness of this electronic auction protocol.

Keywords: Auction, cryptography, security.

1 Introduction

Electronic auction system can be generally classified into two categories. One is called public bid auctions, in which the bidders make public bids on the product; bids must higher than all bids in the previous round of bidding. When nobody submits a new bid in a given round, the product is sold to the highest bidder from the previous round. In this type, bidder may submit many bids for each auction, so it is also called *Multi-bidding* auction. The other type is sealed bid auction. All bids are sealed. When the deadline of the bidding, auctioneer can open the bid and decide the winning bid. Because each bidder can only submit one bid for each auction, we also call it *Single-bidding* auction.

In the existing papers of electronic auction schemes [1, 4, 5, 6, 7, 8, 9, 10], only Subramanian propose a multi-bidding auction scheme [10]. It used the technique of public key cryptosystem to establish a secure transaction channel. This protocol involves an auctioneer, a set of third parties and a set of bidders. The auction house has a product and wants to sell for the highest price offered.

The bidder makes a bid on the product before the end of a bidding period. At the end of a round, the auctioneer collects all the bids and publishes the highest bid. In the next round of bidding, bidder must hike the bid which is higher than the highest bid in the previous round. If no higher bid was offered, the auctioneer publishes the highest price and sells the product.

After the auction, the bidder who offered the highest bid was notified and the bidder had to make a payment (e.q. using credit card or electronic cash [3]) to the auctioneer. It is important the auctioneer cannot duplicate the received payment information.

By using public key cryptography and formal verification, Subramanian showed that the auction protocol ensured the following properties:

1. *Anonymity,* nobody (including the auctioneer) can know the true identity of bidder.

2. *Security,* the integrity and confidentiality of the transaction messages must be protected.

3. *Privacy,* third party cannot know details about the transaction such as payment amount, product details.

4. *Atomicity,* the transaction is either completed or aborted.

5. *Low overhead cost,* the transaction cost must be low enough to suite for transactions involving a small of money.

In this article, we illustrate that the Subramanian's auction protocol has three weaknesses: (1) the bid can be forged by a malicious auctioneer, (2) the sensitive information about payment may be revealed by the auctioneer, and (3) Subramanian's protocol does not resolve the ties between bidders efficiently. By adding time-stamps [2], we will remedy these weaknesses and improve the robustness of Subramanian's electronic auction protocol.

2 Description of Subramanian's electronic auction protocol

In this section, we review the Subramanian's electronic auction protocol [10]. Initially, the protocol notations are defined as follows:

- $''U''$ stands for the auction house, and the auction house's public and private keys are $''u''$ and $''\frac{1}{u}''$, respectively .
- $''B''$ stands for the bidder, and B's public and private keys are $''b''$ and $''\frac{1}{b}''$, respectively.
- $''T''$ stands for the third party, and the third party's public and private keys are $''t''$ and $''\frac{1}{t}''$, respectively.
- $''E''$ and $''e''$ are two encryption keys. $''\frac{1}{E}''$ and $''\frac{1}{e}''$ are two corresponding decryption keys.
- $X \to Y\ :\ [message]^{\frac{1}{x}}$ means that X signs the $''message''$ with $X's$ private key, and sends it to Y. Therefore, Y can verify that the $''message''$ is from X.
- $X \to Y\ :\ [message]^{y}$ means that X encrypts the $''message''$ with $Y's$ public key, and send it to Y. Therefore, only Y can decrypt the $''message''$ with his private key $\frac{1}{y}$.

Subramanian's electronic auction protocol can be divided into three stages: (1) the advertisement stage, (2) the bidding stage, and (3) the exchange of the product and the payment stage. The processes of each stage are described below:

The advertisement stage:

1. $U \rightarrow$ *everybody:* $[product\ description,\ list\ of\ recognized\ third\ parties]^{\frac{1}{u}}$ (M_1);

   For advertising, U first broadcasts the message M_1 which includes product description and a list of third parties that U trusts. The third parties issue pseudo-identities (i.e. public key) to each bidder.

2. $U \rightarrow$ *everybody:* $[product\ identifier,\ product^E]^{\frac{1}{u}}$;

   U also broadcasts the product identifier and the ciphertext of the product which is encrypted with key E; the product identifier is a part of the product description, which is used to prevent the mix-ups with regarding sales of other product. Both the messages are signed with $U's$ private key $\frac{1}{u}$ so that the interested bidders can verify that these messages are from U.

The bidding stage:

1. $B \rightarrow U$: $[M_1,\ b,\ third\ party\ T,\ payment^e,\ [price]^{\frac{1}{b}}]^u$;

   B bids on the product by responding to $U's$ advertisement. The information of the bid includes the message M_1, $B's$ public key, third party T who issued B's public key, the encrypted payment with key e, and the signed price offered by B. U can check the validity of $B's$ public key by looking up the $T's$ directory. Then U can use the public key b to confirm the price is offered from B.

2. $U \rightarrow B$: $[[payment^e]^{\frac{1}{u}},\ [price]^{\frac{1}{b}}\ ]^b$;

   After receiving the bid, U acknowledges the receipt of the bid. The acknowledgement includes the encryption of the payment signed by $U's$ private key $\frac{1}{u}$, and the price signed by $B's$ private key $\frac{1}{b}$. And it is secured with the $B's$ public key b.

3. $U \rightarrow$ *everybody: [product description, maximum price offered]*$^{\frac{1}{u}}$;

   When a round of bidding is cut-off, U collects all the bids in this round and publishes the maximum bid.

   This stage is repeated until no bidder wishes to make a higher bid. The protocol assumes that U can hike the maximum price to expect other bidders for offering more. Furthermore, this method may be used to resolve ties between bidders.

The exchange of the product and the payment stage:

1. $U \rightarrow$ *everybody:* $[product\ description,\ sold\ for\ price]^{\frac{1}{u}}$ (M_2);

   If no higher bid is offered, U publishes the highest bid in this auction and the product is sold for the highest price quoted. The message M_2 is signed by U so that bidders can verify the message from U.

2. $B \rightarrow U$: $[M_2,\ [\frac{1}{e}]^{\frac{1}{b}}]^u$;

   B responds with the signature of decryption key $\frac{1}{e}$ for his payment. If B does not respond, U approaches T with $B's$ bid and collects the payment.

3. $U \rightarrow B$: $[[\frac{1}{e}, \frac{1}{E}]^{\frac{1}{u}}]^b$;

   Finally, U acknowledges the payment and sends the decryption key $\frac{1}{E}$ of the product. The bidding and exchange the product and the payment processes are shown in Fig.1.

In this auction protocol, once a bidder makes the highest bid for an auction, the bidder cannot refuse to buy the product. Third parties act as collection agencies to ensure this feature. If the winner does not respond the decryption key $\frac{1}{e}$ or deliver the wrong payment information, third party can look up the winner's true identity according to his pseudo-identity (i.e. public key). This

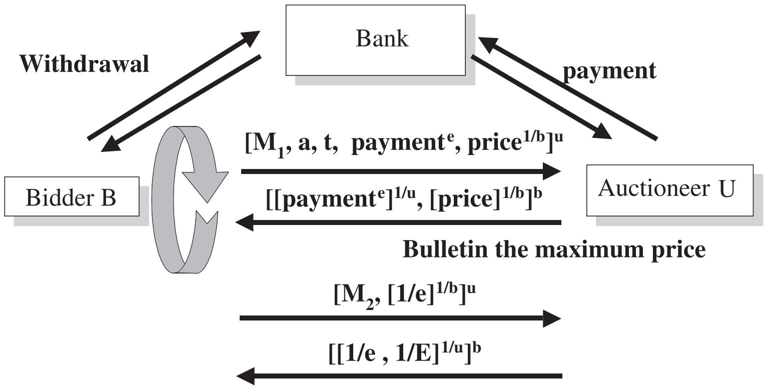

Figure 1: The processes of bidding and exchange the product and the payment in Subramanian's auction protocol

conflicts with anonymity. Therefore, bidders must trust for these third parties do not reveal bidder's identity or other information arbitrarily.

3 The weaknesses of Subramanian's electronic auction protocol

In Subramanian's protocol, Subramanian's auction protocol has the following weaknesses:

1. The bid can be forged by a malicious auctioneer.

   Once receiving a bid from bidder B, a malicious auctioneer can pretend bidder B to make a bid in other auctions. In the step (1) of the bidding stage, auctioneer can obtain the information of b, *third party* T, $payment^e$, and the signature of $[price]^{\frac{1}{b}}$. Therefore, the malicious auctioneer can make an forged bid $[M_1', b, \mathit{third\ party}\ T, payment^e, [price^{\frac{1}{b}}]]^{u'}$ for other auctions, where U' may stand for the same or different auctioneer. The auctioneer U' will convince that the bid is made from B by verifying the signature $[price]^{\frac{1}{b}}$ with $B's$ public key. If B is the winner of the auction, he must pay the payment. Even if the malicious auctioneer does not know the decryption key $[\frac{1}{e}]$ (i.e. no B responds it), U' also can collect the payment through the third party.

2. The sensitive information of payment can be revealed.

   In Subramanian's auction protocol, the existence of some acceptable electronic form of payment such as credit card number, an electronic cash, or any other electronic entity that does not compromise the bidder's privacy or anonymity. However, the information of the payment (e.q. credit card number) can be revealed once the auctioneer received the decryption key from the winner. Furthermore, the malicious auctioneer may reveal the payment information ($[payment^e]'$ and $\frac{1}{e}$) of bidder B_1 to another bidder B_2. Then, B_2 can make a bid that is using the revealing payment information such as $[M_1$, b, $third\ party\ T$, $[payment^e]'$, $[price]^{\frac{1}{b}}]^u$ in another auction. If the bid is the highest bid of the auction, B_2 responds the the decryption key $\frac{1}{e}$ to the auctioneer. Hence, bank will collect the payment from B_1, not from B_2.

3. The ties between bidders do not be resolved efficiently.

   The auction protocol may be stuck in a situation that the highest bid for a product is offered by more than one bidder. The resolution of this conflict is using some agents to hike the maximum bid artificially. However, if no bidder makes higher bid than the agent's, what shall the auctioneer do?

4 The revised protocol

In this section, we modify Subramanian's auction protocol to improve the robustness of the protocol. The revised protocol is similar to Subramanian's auction protocol, except for the following modifications.

In the step (1) of the bidding stage, we add timestamp TS to the electronic form of payment and price so that the step becomes

$$B \rightarrow U : [M_1,\ b,\ third\ party\ T,\ bank\ K,\ TS,\ [[TS \oplus payment]^e]^k,\ [TS \oplus price]^{\frac{1}{b}}]^u;$$

where TS is a timestamp, k is the public key of bank K, and $\oplus$ denotes an operation of exclusive OR. With the payment encrypted with k, the auctioneer will not be able to know the payment information. With the form of $[TS \oplus payment]$, the auctioneer cannot replay the payment, once TS is expired. Auctioneer is still able to validate the payment by sending this message to bank.

When U received the bid at the time TS', it checks the correctness of the timestamp first. Let ΔT denote the expected legal time interval for transmission delay between the bidder's terminal and the auctioneer's server. If the time interval between TS and TS' is greater than ΔT ($TS' - TS > \Delta T$), U shall reject the bid.

Then, U acknowledges the receipt of the bid in step (2) of this stage and the delivered message now becomes

$$U \to B: \ [[[[TS \oplus payment]^{e}]^{k}]^{\frac{1}{u}}, \ [TS \oplus price]^{\frac{1}{b}}]^{b}.$$

When the time allotted for a round of bidding is expired, U bulletins the maximum bid. In step (3) of bidding stage, TS has to be published along with the publication, thus, the step becomes:

$$U \to everybody: \ [product\ description, \ TS, \ maximum\ price\ offered]^{\frac{1}{u}}.$$

When no bidder makes a higher bid for the product, U notify each bidder about the sold for price. Adding timestamp, the step becomes:

$$U \to everybody: \ [product\ description, TS, sold\ for\ price]^{\frac{1}{u}}.$$

When the highest bid for a product is offer more than one bidder, the bid with lower timestamp will win the bid. Now, auctioneer can determine who is the winner based on the timestamp. And this case resolves the conflicts that generally happen in the real world auction sites.

After U publishes the price for sold, the winner responds the deciphering key for his payment. However, it is now different from Subramanian's auction

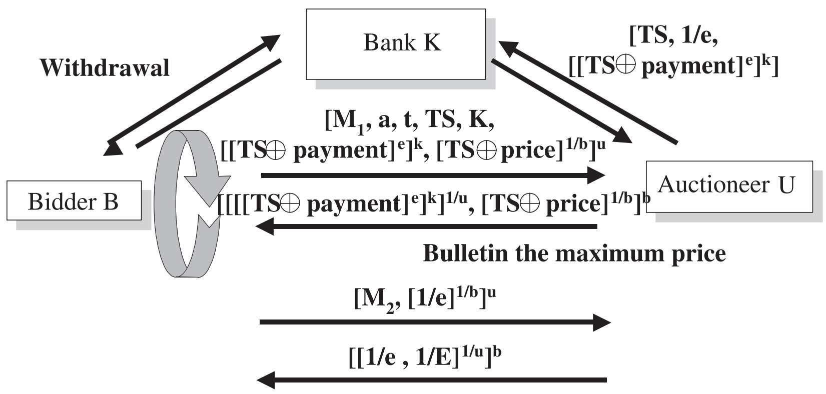

Figure 2: The processes of bidding and exchange the product and the payment in our auction protocol

protocol in that U cannot longer decrypt the message of this payment and has to forward the encrypted payment information, the deciphering key $\frac{1}{e}$, and the TS to the bank K for reimbursement. The bank can obtain the payment information by

$$[[[TS \oplus payment]^e]^t]^{\frac{1}{t}} = [TS \oplus payment]^e, \tag{1}$$

$$[[TS \oplus payment]^e]^{\frac{1}{e}} = [TS \oplus payment], \tag{2}$$

$$[TS \oplus payment] \oplus TS = payment. \tag{3}$$

The processes of bidding and exchange the product and the payment in our proposed protocol are shown in Fig.2.

Security Analysis

In our revised protocol, we resolve the three weaknesses of Subramanian's auction protocol. Firstly, we add timestamp to the price and sign it with bidder's secret key. The auctioneer can computer the price using the bidder's public key and timestamp TS from the following equation:

$$price = [[TS \oplus price]^{\frac{1}{b}}]^b \oplus TS. \tag{4}$$

Only the bidder knows the secret key, hence auctioneer cannot forge the signature of $[TS \oplus price]$. If the auctioneer replays the message to another auction, the verification of timestamp will fail. Therefore, the weakness (1) is eliminated.

Secondly, we add timestamp to the payment and encrypt the message $[[TS \oplus payment]^e]$ with bank's public key. Without bank's secret key, auctioneer cannot decrypt the message. Therefore, the sensitive information can be protected. Furthermore, the payment information is exclusive OR with TS, hence the scenario of describing in weakness (2) is not happening. The auctioneer will check the timestamp firstly.

Thirdly, when two or more bidders offer the same bid and the bid is the highest of this round, comparing their timestamp, the lowest timestamp will be the winner. However, if a bidder wants to choose the lower timestamp, the bid may not pass the verification $TS' - TS \leq \Delta T$.

5 Conclusions

A secure electronic auction protocol is very important in modern electronic markets. It advances the commerce of auction full of vitality. In this article, we propose an extension of Subramanian's auction protocol. The main advantages of our revised protocol are:

- any malicious auctioneer cannot forge a bid or replay the payment,
- it prevents the payment information from leaking out, and
- it improves the robustness of Subramanian's protocol by increasing privacy and conflict resolution.

Acknowledgements

The authors wish to thank many anonymous referees for their suggestions to improve this paper. This research was partially supported by the National Science Council, Taiwan, R.O.C., under contract no.: NSC89-2213-E-324-053.

References

[1] M.K. Franklin and M.K. Reiter, "The design and implementation of a secure auction service," *IEEE Transactions On Software Engineering*, vol. 22, pp. 302–312, MAY 1996.

[2] M.S. Hwang, W.G. Tzeng, and W.P. Yang, "A two-key-lock-pair access control method using prime factorization and time stamp," *IEICE Transactions on Information and Systems*, vol. E77-D, no. 9, pp. 1042–1046, 1994.

[3] M.S. Hwang, I.C. Lin, and L.H. Li, "A simple micro-payment scheme," *International Journal of Systems and Software*, vol. 55, no. 3, pp. 221–229, 2001.

[4] S. Inoue and T. Matsumoto, "A note on anonymous electronic auction," *IEICE Technical Report, Information Security*, vol. ISEC 95-5, 1995.

[5] T. Kawagoe, "Electronic auction mechanism," *Proc. Symposium on Information Media'96*, pp. 75–82, 1996.

[6] H. Kikuchi, M. Hakavy, and D. Tygar, "Multi-round anonymous auction protocols," *IEICE Trans. on Information and Systems*, vol. E82-D, no. 4, pp. 769–777, 1999.

[7] M. Kudo, "Secure electronic sealed-bid auction protocol with public key cryptography," *IEICE Trans. On Fundamentals*, vol. E81-A, no. 1, pp. 20–27, 1998.

[8] T. Nakanishi, II. Watanabe, T. Fujiwara, and T. Kasami, "Undeniable electronic anonymous bidding protocol," *IEICE Technical Report, Information Security*, vol. ISEC 94-3, 1994.

[9] H. Nurmi, "Cryptographic protocols for auctions and bargaining," *Proc. of Results and Trends in Theoretical Computer Science*, pp. 317–324, 1994.

[10] S. Subramanian, "Design and verification of a secure electronic auction protocol," *IEEE 17th Symposium on Reliable Distributed Systems*, pp. 204–210, 1998.

M.-S. Hwang received the B.S. in Electronic Engineering from National Taipei Institute of Technology, Taipei, Taiwan, Republic of China, in 1980; the M.S. in Industrial Engineering from National Tsing Hua University, Taiwan, in 1988; and the Ph.D. in Computer and Information Science from National Chiao Tung University, Taiwan, in 1995. He also studied Applied Mathematics at National Cheng Kung University, Taiwan, from 1984-1986. Dr. Hwang passed the National Higher Examination in field "Electronic Engineer" in 1988. He also passed the National Telecommunication Special Examination in field "Information Engineering", qualified as advanced technician the first class in 1990. From 1988 to 1991, he was the leader of the Computer Center at Telecommunication Laboratories (TL), Ministry of Transportation and Communications, ROC. He was also a project leader for research in computer security at TL in July 1990. He obtained the 1997, 1998, and 1999 Distinguished Research Awards of the National Science Council of the Republic of China. He is currently a professor and chairman of the Department of Information Management, Chaoyang University of Technology, Taiwan, ROC. He is a member of IEEE, ACM, and Chinese Information Security Association. His current research interests include database and data security, cryptography, image compression, and mobile communications.

Eric Jui-Lin Lu received his B.S. degree in Transportation Engineering and Management from National Chiao Tung University, Taiwan, R.O.C, in 1982; M.S. degree in Computer Information Systems from San Francisco State

University, California, U.S.A, in 1990; and Ph.D. degree in Computer Science from University of Missouri-Rolla, Missouri, U.S.A, in 1996. He is currently an associate professor of the Department of Information Management and Director of Computer Center, Chaoyang University of Technology, Taiwan, R.O.C. His current research interests include electronic commerce, distributed processing, and security.

I.-Ch. Lin received the B.S. in Computer and Information Sciences from Tung Hai University, Taichung, Taiwan, Republic of China, in 1998; the M.S. in Information Management from Chaoyang University of Technology,Taiwan, in 2000. He is currently pursuing his Ph.D. degree in Computer Science and Information Engineering from National Chung Cheng University. His current research interests include electronic commerce, information security, cryptography, and mobile communications.