A Simple Efficient Electronic Auction Scheme

Wen Chen and Feiyu Lei
Department of Communications and Electronic Engineering,
School of Information Science and Technology, Donghua University,
1882 Yanan Road, Shanghai, China, 200051
wen.chenwen@gmail.com

Abstract

This paper proposes a new simple efficient electronic auction scheme based on quadratic residue. Our scheme satisfies the basic security requirements for a sealed-bid auction system.

1. Introduction

Electronic Auction has been a major topic of electronic commence in the recent years. There are a variety of auction styles such as English, Dutch, Sealed-Bid etc.[2] Our target among the auction styles is to design the Sealed-Bid auction in which a bidder commits his bid with which he is willing to pay on the items without disclosure of the bidding price, then after the bidding session, the auctioneers open the received bids and declare the highest bid as the winning price and the winner who sent the highest bid. In most of previous schemes[2, 3], each bidder issues an encrypted bidding price or commitment of bid. However, they are unefficient to be reasonable for implementation. Motivated by this, we propose a simple efficient electronic auction scheme, which provides some basic security requirements in the literature [2, 3].

2. Quadratic Residue

Quadratic Residue [5]: Let n be an integer (Note: In this paper, we assume that it is infeasible to factorize n.), $a \in Z_n^*$ is said to be a quadratic residue modulo n, if there exists an $x \in Z_n^*$ such that $x^2 \equiv a \, mod \, n$. If no such x exists, then a is called a quadratic non-residue modulo n. The set of all quadratic residues modulo n is denoted by Q_n and the set of all quadratic non-residues modulo n is denoted by $\widetilde{Q_n}$. Let p be an odd prime and a an integer. The Legendre symbol $(\frac{a}{p})$ is defined to be:
Case0:$(\frac{a}{p}) = 0$ if $p|a$,
Case1:$(\frac{a}{p}) = 1$ if $a \in Q_p$,
Case2:$(\frac{a}{p}) = -1$ if $a \in \widetilde{Q_p}$.
The Jacobi symbol $(\frac{a}{n})$ is a generalization of the Legendre symbol to integers n which are odd but not necessarily prime.

Fact1: Let n be a product of two distinct odd primes p and q. Then $a \in Z_n^*$ is a quadratic residue modulo n if and only if $a \in Q_p$ and $a \in Q_q$.

Fact2: n is a Blum integer if $n = pq$ and (p, q) are distinct odd primes such as $p \equiv q \equiv 3 \; mod \; 4$. Then $(\frac{-1}{p}) = (\frac{-1}{q}) = -1$. So we can easily generate a number $w \in Q_n$ or a number $r \in \widetilde{Q_n}$ as follows: firstly random choose an integer e, then compute $w = e^2 \; mod \; n$,$r = -w \; mod \; n$.

3. The Proposed Sealed Bid Auction Scheme

Preparation: Let $\{A_i | i = 1, 2, ..., a\}$ be auctioneers and $\{B_j | j = 1, 2, ..., b\}$ be bidders, a Seller $\mathcal{S}$. The seller publishes a price list $P = \{j | j = 1, 2, ..., u\}$. The auctioneers publish a great Blum integer $N = pq$, and keep (p, q) as secrets. Then we use a known sharing secret technique [1] to distribute p and q among the auctioneers.

1. Choose $p_1, q_1, ..., p_l, q_l \in_R (0, 2^{2n})$ such that $p_i = q_i = 0 \; mod \; 4$, for all i
2. Set $p_0 = p - \sum_{i=1}^{l} p_i$ and $q_0 = q - \sum_{i=1}^{l} q_i$
3. Send (p_i, q_i) to A_i
4. Broadcast (N, p_0, q_0)

Bidding: Bidder B_i decides his bidding price $p_i \in P$, and computes his bidding vector as remarked in Section 2.

$$C_{i,j} = \begin{cases} choose \quad an \quad integer \quad r_j \in \widetilde{Q_N} if j = p_i & , \\ choose \quad an \quad integer \quad r_j \in Q_N if j \neq p_i & , \end{cases}$$

He publishes the sequence of numbers $(C_{i,1}, C_{i,2}, ..., C_{i,u})$ and his signature on the sequence. When the bidding phase

0-7695-3049-4/07 $25.00 © 2007 IEEE
DOI 10.1109/.60

is ended, we get the matrix as follows:

$$\begin{matrix} C_{1,1} & C_{1,2} & ... & C_{1,u} \\ C_{2,1} & C_{2,2} & ... & C_{2,u} \\ ... & ... & ... & ... \\ C_{b,1} & C_{b,2} & ... & C_{b,u} \end{matrix}$$

Opening: Firstly, we may decide whether a number C is a quadratic residue by computing the following algorithm [1]:

$\diamondsuit$ Begin Algorithm-QRflag(C) $\diamondsuit$

1. All auctioneers compute the Jacobi symbol $(\frac{C}{N})$. If $(\frac{C}{N}) \neq 1$, all auctioneers output $\perp$ and stop
2. Otherwise $(\frac{C}{N}) = 1$, the auctioneer A_i broadcasts $b_i = C^{(-p_i-q_i)/4} \ mod \ N$
3. all auctioneers compute $b_0 = C^{(N-p_0-q_0+1)/4} \ mod \ N$
4. all auctioneers compute $QRflag = (1 - \prod_{i=0}^{l} b_i \ mod \ N)/2$, returns $QRflag$.

$\diamondsuit$ End Algorithm-QRflag(C) $\diamondsuit$

Then in the opening phase, all auctioneers perform the following program, and use above Algorithm-QRflag as a subroutine:

$\diamondsuit$ Begin Opening$\diamondsuit$
for $k = u$ to 1
for $t = b$ to 1
if Aglorithm-QRflag$(C_{t,k}) = 1$ then
return $Winner = B_t, Price_{win} = k$
$\diamondsuit$ End Opening $\diamondsuit$
As a result, the winner is B_t, and the winning price is k.

4. Analysis of the Proposed Scheme

4.1. Security

Secrecy of bidding price : It is difficult to estimate whether an integer is a quadratic residue modulo N when N is a large composite integer whose prime factors are unknown. Furthermore, the Jacobi symbols of all $C_{i,j}$ are equal to 1. So the adversary cannot know the bidding price of B_i. Besides, all auctioneers do the opening actions in a threshold setting. When the winner is decided, the opening phase is ended. That is to say, for each auctioneer, the opening action doesn't compromise any valid information about the bidding price. Therefore, it is secure under the quadratic residuosity assumption [1, 4]

Public verifiability: Firstly, anyone can compute the Jacobi symbol of all $C_{i,j}$. If $(\frac{C_{i,j}}{N}) = -1$, the bidding vector is invalid. Secondly, since the bidding vector $C_{i,j}$ is signed by bidder B_i, no one except bidder B_i himself can modify or forge the bidding vectors and share them. So anyone can verify the correctness of the auction by checking the validity of these bidding vectors and signatures.

Robustness: A corrupted bidder B_i may generate a invalid vector $C_{i,1}, C_{i,2}, ..., C_{i,u}$ such as at least two $C_{i,j} \in \widetilde{Q_N}$. But if he wins the auction, he should pay the highest price according to his bidding vector. So it is still correct for the whole system, and the corrupted B_i can't gain any benefits from his invalid vector.

4.2. Efficiency

Most previous electronic auction schemes [2, 3] need to compute too much complicated modular exponentiations, and the communication cost is also high for *Robustness* and *Public verifiability*.

The proposed scheme can be performed very efficiently, which only needs to compute the Legendre and Jacobi symbols in bidding phase, and a few modular exponentiations in opening phase. And as discussed in Section 4.1, the scheme has a low communication cost for *Robustness* and *Public verifiability*, and doesn't need additional communication any more.

5. Conclusion

We have pointed out the previous electronic sealed-bid auctions are not efficient enough for the real life, whereas the proposed scheme enjoys secrecy of bidding price, robustness and public verifiability, and can be performed efficiently.

References

[1] J. K. Author. Threshold cryptosystems based on factoring. *ASIACRYPT 2002*, Lecture Notes in Computer Science 2501:192–205, 2002.

[2] K. O. Author. A study on electronic auctions. *Ph.D Thesis, School of information science, Japan Advanced Instititue of Sicence and Technology*, 2002.

[3] M. A. Author. Receipt-free sealed-bid auction. *5th International Conference on Information Security table of contents,ISC 2002*, Lecture Notes in Computer Science 2433:191 –199, 2002.

[4] S. G. Author. Probabilistic encryption and how to play mental poker keeping secret all partial information. *14th ACM Symposium on the Theory of Computing*, pages 365–377, 1982.

[5] A. J. M. Expert. *Handbook of applied cryptography*. CRC Press, New York, 1997.