
Efficient Receipt-Free Electronic Auction Protocol

Huang, Zheng

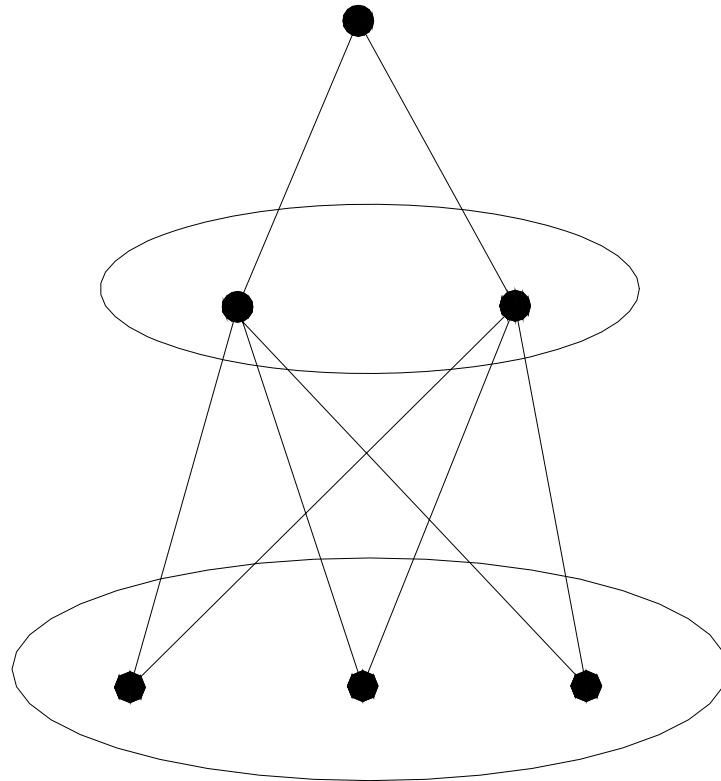
Institute of Information Security
Shanghai Jiaotong University

Receipt-Free Auction

Abe and Suzuki first propose the concept of Receipt-Free auction protocol that eliminates “receipts” to prevent bid-rigging .

The proposed protocol in requires a bidding booth and a one-way untappable channel from each bidding booth to each auctioneer.

Auction Model



Seller

Auctioneers

Bidders

Requirements for auction

- *Correctness*
- *Non-repudiation*
- *Secrecy of bidding price*
- *Public Verifiability*
- *Receipt-freeness* : Anyone, even the bidder himself, must not be able to prove any information about the bidding price except what can be found from the result of the auction.

Protocol proposed

The protocol is based on Abe's protocol. The contribution of this paper is that :

- Use chameleon bit-commitment to commit on every bits of the bidding price.
- Design an algorithm to open the sealed bids.

Overview of the protocol

1. Setup Phase
2. Bidding Phase
3. Opening Phase

Setup Phase

In the setup phase, the system chooses a generator g from G_q in Z_p^* and g is an element of order q , where p and q are two primes such that $p = 2q + 1$, G_q is the group generated by g , and Z_p^* is a finite field. The system also selects two values $M_0, M_1 \in Z_q$ that mean “this bit is 0”, “this bit is 1” respectively. Each bidder B_j selects his secret key $x_j \in Z_q$ of chameleon bit-commitment and publish his public key $h_j = g^{x_j}$.

Bidding Phase

The Bidder :

1. Generate the Commitments as

$$C_{l,j} = \begin{cases} g^{n,j} g^{M_1} h_j^{n,j} & (v_l = 1) \\ g^{n,j} g^{M_0} h_j^{n,j} & (v_l = 0) \end{cases} \quad (\text{for } l = 1, \dots, m)$$

2. Publish the commitments.
3. Zero-Knowledge proof the commitments are well formed.
4. Share the random number among the auctioneers

Opening Phase

The Auctioneers, From High bit to Low bit, do the following :

1. Reconstruct the random number.
2. Open the Commitments.
3. Modify the winner set until the size of the set is 1.

The End , Thank you.